Joint Pub 2-01

Joint Intelligence Support to Military Operations

20 November 1996

PREFACE

1. Scope

This publication establishes doctrinal guidance on the provision of intelligence products, services, and support to joint operations. It provides the fundamentals of joint intelligence operations, addressing organization of joint intelligence forces, responsibilities, and command relationships. The focus will be joint intelligence support to combatant commanders revolving around the phases of the intelligence cycle: planning and direction, collection, processing and exploitation, production; dissemination and integration and evaluation. Finally, personnel, physical, operations and communications security considerations will be addressed.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth doctrine to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes doctrine for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the joint force commander (JFC) from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. Doctrine and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. The guidance in this publication is authoritative; as such, this doctrine (or JTTP) will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

For the Chairman of the Joint Chiefs of Staff:

DENNIS C. BLAIR
Vice Admiral, US Navy
Director, Joint Staff

Intentionally Blank

TABLE OF CONTENTS

Table of Contents

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses the Role of Intelligence in Military Operations**
- **Covers Joint Intelligence Planning**
- **Outlines the Intelligence Cycle**
- **Explains Intelligence Command, Control, Communications, and Computer Systems Support**

The Role of Intelligence in Military Operations

The objective of joint intelligence operations is to provide the joint force commander with a timely, complete, and accurate understanding of the adversary and the environment.

Joint intelligence doctrine defines the roles and relationships of intelligence organizations at the national level, in the combatant commands, and in the subordinate joint forces. The goal is to **maximize the impact of intelligence** while increasing effectiveness among the organizations that support the joint force commander (JFC). Intelligence plays a critical role across the range of military operations from peace to war. **Intelligence enables commanders at all levels to focus their combat power and resources** and to provide force protection for those resources. Operations associated with military operations other than war focus on deterring war and promoting peace and can have rules of engagement requiring the adaption of a new and complex set of operational responses. **Intelligence resources at every echelon should be structured to provide support that is proactive, aggressive, predictive, and flexible.** Successful conduct of information warfare operations also demands detailed intelligence support.

Joint Intelligence Planning

The planning effort must be focused to ensure that it is responsive to the commander's requirements and the requirements of subordinate units and/or elements.

The essence of effective planning is the **full definition of the mission, expression of the commander's intent, completion of the commander's estimate** (including the intelligence estimate), and **development of a concept of operations** with an intelligence annex. The Command Intelligence Architecture and/or Planning Program is a systematic and structured planning process that documents the combatant command's mission linkage to intelligence requirements, current and required future intelligence capabilities, and intelligence missions and organization.

The different planning processes involved are deliberate,

The **deliberate planning process is primarily conducted in peacetime** and engages the entire joint planning community in the methodological development of plans for all contingencies, and the transition to and from war. Deliberate planning consists of **five phases:** initiation, concept development, plan development, plan review, and supporting plans.

crisis action planning,

Crisis action planning (CAP) procedures provide for the transition from planning military operations to actual execution through the timely flow of intelligence, rapid execution of military options, and the timely relay of decisions of the National Command Authorities to supported commanders. Crisis action planning and execution are accomplished within a framework of **six phases:** situation development, crisis assessment, course of action (COA) development, COA selection, execution planning, and execution.

and campaign planning.

Campaign planning is appropriate when military operations exceed the scope of a single major operation. **It encompasses both the deliberate and CAP processes.** Intelligence supports all aspects of the campaign plan. A campaign plan describes how a series of operations are arranged in time, space, and purpose. The plan focuses on the adversary's centers of gravity; simultaneous and synchronized employment of land, sea, air, space-based, and special operations forces assets; and the end state to be achieved.

The Intelligence Cycle

The intelligence cycle focuses on the commander's mission and concept of operation.

Each phase of the cycle must be synchronized with the commander's decision making and operational requirements to successfully influence the outcome of the operation. **The intelligence cycle provides a process to understand and order the many activities involved in intelligence** and is useful for understanding the interrelationships of the intelligence phases. The intelligence process may not continue through the entire cycle and there are no firm boundaries delineating where each phase of the cycle begins or ends. **Activities during each phase of the intelligence cycle directly support the JFC.** Intelligence supports joint operations, focusing on providing multidiscipline intelligence support to the combatant command, the subordinate Service and functional component commands, and the subordinate joint force.

The six phases of the intelligence cycle are Planning and Direction,

While conducted continuously, **intelligence planning and direction normally occurs during and in conjunction with operation planning** and involves task-organizing intelligence assets; identifying personnel, logistics and communications requirements; developing a collection plan; issuing requests for collection and production; and monitoring the availability of collection information.

Collection,

Collection operations acquire information about the adversary and provide that information to intelligence processing and exploitation elements. Collection management converts intelligence requirements into collection requirements; establishes, tasks, or coordinates actions with appropriate collection sources or agencies; and monitors results and retasks, as required. Requests for collection resources must be coordinated with the echelon that directs and controls them through the chain of command. **Collection managers develop collection plans based on the intelligence requirements of commanders and decision makers** and should observe the following principles in all collection considerations: early identification of requirements, prioritization of requirements, multidiscipline approach, and task organic assets. **Collection management has two distinct functions: defining what intelligence systems must collect, and specifying how to collect it.** Management and validation of collection requirements requests for a theater resides at the component and/or combatant command.

Processing and Exploitation,

During processing and exploitation, collected data is correlated and converted into forms suitable for analysis and production which may be further exploited to gain fullest possible advantage from it. The exploitation manager must plan the workload and develop a priority system for accomplishing the work. This will ensure priority processing and exploitation during periods of high-volume collection activity.

Production,

Intelligence production is the integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence. Production for joint operations is accomplished by organizations at every echelon, from national to joint force level. Intelligence products produced by or for the subordinate joint force are indications and warning, current intelligence, general military intelligence, and target intelligence. **Production centers at all levels are assigned clearly delineated areas of analytical responsibility across the range of military operations.**

Dissemination and Integration,

Intelligence must be provided in a form that is readily understood and directly usable by the recipient in a timely manner without overloading the user and minimizing the load on communications capabilities. **Dissemination consists of both "push" and "pull" control principles.** The "push" concept allows the higher echelons to push information down to satisfy existing lower echelon requirements or to relay other relevant intelligence to the lower level. The "pull" concept involves direct electronic access to data bases, intelligence files, or other repositories by intelligence organizations at all levels. **The requester must integrate all intelligence obtained from national, theater, or organic resources and/or assets into the decision making and planning process.**

and Evaluation.

The intelligence cycle is evaluated at every phase to determine the success achieved in meeting the customer's requirements. The planning and direction phase depends on the results achieved in the other phases of the intelligence cycle. The collection manager evaluates the collection report(s), ensures that the requesters receive a copy, and determines if the requirement has been satisfied. Requester feedback establishes customer satisfaction and frees collection assets and resources to be redirected to satisfy other active requirements. The processing and exploitation ("sensor" specific) and production (multiple sensors or sources) phases are evaluated based on customer satisfaction with the product provided in response to a request. Intelligence personnel at all levels evaluate the production process and the products in an effort to continuously improve support to the requester. Intelligence personnel at all levels assess the success of the dissemination and integration phase of the intelligence cycle and make changes as needed to improve the process.

Intelligence Command, Control, Communications, and Computer Systems Support

Communications and automated data processing technology is undergoing continuous evolution, affecting intelligence architecture, systems, and applications.

Communications and automated data processing (ADP) systems provide the basic framework for the timely movement and transfer of information in each phase of the intelligence cycle to commanders and other key decision makers. Joint intelligence, national agency communications support, and multinational force intelligence and communications help with command, control, communications, and computer systems support. **Key concepts** of successful intelligence systems are **joint interoperability, streamlined flow of information**, and **providing pull-down of intelligence tailored to the needs of the operating forces**. Combatant commanders'

communication planning consists of architecture planning and system planning.

Joint intelligence architecture implements common procedures, standards, and streamlined support.

The **joint intelligence architecture** encompasses both the Joint Worldwide Intelligence Communications System, the Joint Deployable Intelligence Support System, and other client-server environment compliant workstations. The **communications and ADP systems and networks** include the Automatic Digital Networks, the Department of Defense Intelligence Information System, the Secret Internet Protocol Router Network, Global Command and Control System, Global Broadcast Service, Migration Defense Intelligence Threat Data System, Military Intelligence Integrated Data System and Integrated Data Base, Joint Collection Management Tools, and the Requirements Management System.

CONCLUSION

Joint intelligence enables commanders at all levels to focus and protect their combat power and resources through a synchronized cycle of planning and direction, collection, processing and exploitation, production, dissemination and integration, and evaluation. Successful intelligence systems must include joint interoperability, a streamlined flow of information, and provide a pull-down of intelligence tailored to the needs of the operating forces.

Intentionally Blank

CHAPTER I
THE ROLE OF INTELLIGENCE IN MILITARY OPERATIONS

"When I took a decision, or adopted an alternative, it was after studying every relevant — and many an irrelevant -— factor. Geography, tribal structure, religion, social customs, language, appetites, standards — all were at my finger-ends. The enemy I knew almost like my own side. I risked myself among them a hundred times, to learn."

Colonel T.E. Lawrence
Letter to Liddell Hart, 26 June 1933

1. Introduction

a. **The objective of joint intelligence operations is to provide the joint force commander (JFC) with a timely, complete, and accurate understanding of the adversary and the environment.** Intelligence staffs must understand the intelligence requirements of their superior and subordinate commands and components, identify organic intelligence capabilities and shortfalls, access theater and/or national systems to alleviate shortfalls, and ensure that timely and appropriate intelligence is provided or available to the JFC and subordinate commands and components. (Figure I-1) **This**

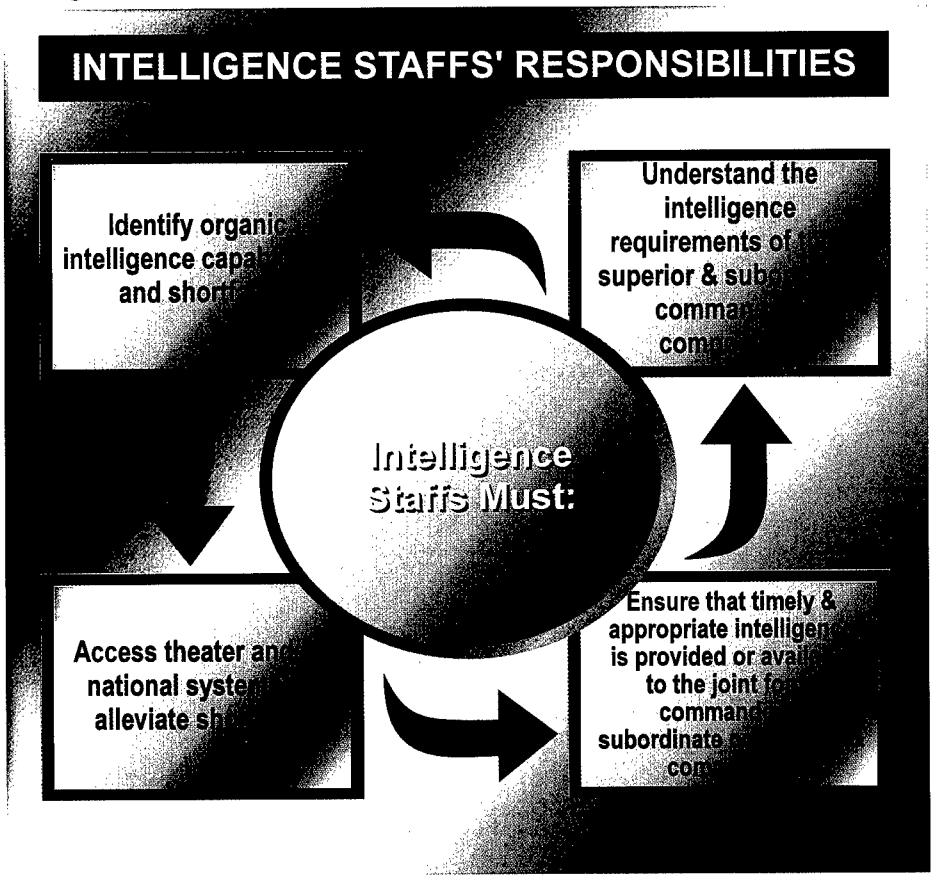
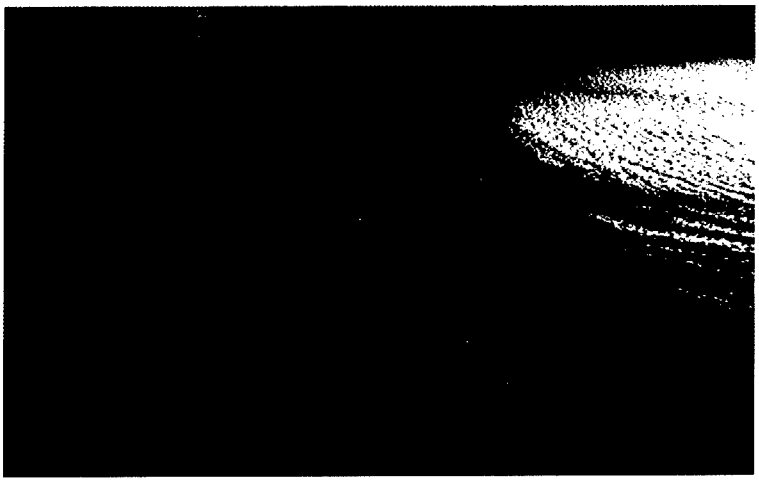


Figure I-1. Intelligence Staffs' Responsibilities

objective is achieved through the cooperative and comprehensive efforts of all intelligence personnel during each phase of the intelligence cycle.

Counterintelligence (CI) plays a key force protection role during war and especially in military operations other than war (MOOTW). An effective CI program uses a multidisciplined approach to counter an adversary's all-source intelligence and other security threats. CI elements from the Service components play a lead role in this multidisciplined effort, conducting the four CI functions of operations, investigations, collection, and analysis. CI elements also complement the intelligence disciplines through functions such as analysis and collection. Additional information on CI support to operations can be found in Joint Pub 2-01.2, "Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations."

b. **Joint intelligence doctrine defines the roles and relationships of intelligence organizations at the national level, in the combatant commands, and in subordinate joint forces.** The National Military Joint Intelligence Center (NMJIC), the combatant command intelligence officer (J-2) and the Joint Intelligence Center (JIC), and the subordinate joint force J-2 and Joint Intelligence Support Element (JISE) support the commander by minimizing the number of organizations and echelons upon which the JFC must rely in order to accomplish intelligence support missions. **The goal is to maximize the impact of intelligence while increasing effectiveness among the organizations that support the JFC.** Robust intelligence resources, methodologies, and products should be developed, reviewed, and exercised regularly to directly support every military option and scenario. Significant opportunities and vulnerabilities across the spectrum of military operations are created as the United States and its adversaries become increasingly dependent on information, information-based processes, and information systems. Information superiority, achievement of dominance in the information environment, is critical if the United States is to maintain dominance. Information warfare (IW), affecting adversary information capabilities while protecting our own, requires detailed intelligence support.



Intelligence helps the combatant commander understand the area of responsibility and visualize and develop the battlespace.

2. Intelligence Operations in War

a. **Intelligence plays a critical role across the range of military operations from peace to war.** Commanders use intelligence to anticipate the battle, understand the battlespace, and influence the outcome of operations. **Intelligence enables commanders at all levels to focus and protect their combat power and resources and provide force protection for those resources.**

b. Intelligence focuses on the adversary centers of gravity to provide operational and tactical commanders the information they need to conduct the campaign. Multidisciplined intelligence gives the commander the information necessary to successfully plan and execute military operations. Intelligence helps the combatant commander and/or subordinate JFC understand the operational area and visualize and develop the battlespace. Intelligence shows where the commander should apply combat power to exploit adversary vulnerabilities or capitalize on opportunities with minimum risk. Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations," describes intelligence and the range of military operations.

3. Intelligence in Military Operations Other Than War

a. **Operations associated with MOOTW focus on deterring war and promoting peace, are very sensitive to political considerations, and can have rules of engagement requiring the adaptation of a new and complex set of operational responses.** The J-2 must modify and tailor the intelligence response to meet the unique challenges presented in each operation. In addition, the nature and intensity of a potential threat in MOOTW can change suddenly and dramatically. For example, a peacekeeping operation may abruptly transition to a combat peace enforcement operation should any of the belligerents fail to honor the terms of the truce. Therefore, **intelligence** resources at every echelon should be structured to provide support that is **proactive, aggressive, predictive, and flexible**. A significant amount of intelligence resources are dedicated to supporting joint organizations with a counterdrug mission. Although counterdrug operations develop rapidly, planning occurs over an extended planning cycle. Counterdrug operations must take into account the special legal, operational, and coordination constraints of counterdrug policy.

b. Rapid and continuing advances in information technology present US forces with significant opportunities and vulnerabilities. A growing percentage of intelligence manpower, technical resources, products and efforts will be dedicated to IW activities that attack, protect or exploit information.

ENVIRONMENTAL DEFENSE INTELLIGENCE

In 1992 the Defense Intelligence Agency sought to improve support for future disaster relief operations. The initiative was largely a response to Operation SEA ANGEL, a major disaster relief operation in Bangladesh in May 1991 in which some 152,000 people were killed by a tropical cyclone. Interviews with SEA ANGEL commanders indicated they had not had adequate intelligence on Bangladesh's physical and cultural environment, infrastructure, disaster relief capabilities, and the potential for further disaster. The DIA initiative attempted to satisfy these requirements in preparing for disasters.

The most important component of this initiative was the development of a new, all-source, comprehensive finished intelligence product modeled on DIA's Contingency Support Studies (CSS) and Contingency Support Products. Such products originally were designed to provide "off-the-shelf" contingency intelligence for combat operations and noncombatant evacuation operations.

The new CSS-type product was designed for potential future humanitarian relief operations generated by natural or technological disasters. In addition to the traditional Essential Elements of Information (EEI) included in studies that support the movement and deployment of military forces — such as transportation infrastructure intelligence — the product was designed to include EEIs that are unique and yet critical to the planning and prosecution of disaster relief operations.

SOURCE: G. Ted Constantine, Intelligence Support to Humanitarian-Disaster Relief Operations, Center for the Study of Intelligence, December 1995

CHAPTER II
JOINT INTELLIGENCE PLANNING

"If I always appear prepared, it is because before entering on an undertaking, I have meditated for long and foreseen what may occur."

Napoleon Bonaparte

1. Introduction

a. **The essence of effective planning is the full definition of the mission, expression of the commander's intent, completion of the commander's estimate (including the intelligence estimate), and development of a concept of operations with Annex B (Intelligence). The planning effort must be focused to ensure that it is responsive to the commander's requirements and the requirements of subordinate units and/or elements.** Sharing operational, communications and intelligence information among the J-2, operations officer (J-3), logistics officer (J-4), plans officer (J-5), and command, control, communications, and computer (C4) systems officer (J-6) staffs is essential.

b. Joint operation plans include deliberate plans and crisis action plans. The planning cycle continues by maintaining and updating plans, as required, until the plan task is canceled. Deliberate plans include operation plans in complete format (OPLANs), operation plans in concept format (CONPLANs) with or without time-phased force and deployment data (TPFDD), and functional plans. Crisis action planning (CAP) is conducted for the actual commitment of allocated forces, based on the current situation, when a contingency response is imminent. This planning results in time-sensitive development of joint operation plans (campaign plans) and/or operation orders (OPORDs) for execution.

c. The Joint Pub 5 series provides detailed information on planning joint operations. The Joint Operation Planning and Execution System (JOPES) provides the means to respond to emerging crisis situations or transition to war through rapid, coordinated execution planning and implementation. JOPES translates policy decisions into OPLANs and OPORDs. JOPES formats can be found in CJCSM 3122.03, "Joint Operation Planning and Execution System Vol II: (Planning Formats and Guidance)," and CJCSM 3122.04, "Joint Operation Planning and Execution System Vol II: (Supplemental Planning and Execution Formats and Guidance)."

d. **The Command Intelligence Architecture/ Planning Program (CIAP) is a systematic and structured planning process that documents the combatant commands' mission linkage to intelligence requirements, current and required future intelligence capabilities, and intelligence missions and organization.** The CIAP addresses the combatant commands' baseline capabilities and objective architectures and identifies shortfalls impeding realization of the objective intelligence architecture. The CIAP addresses interoperability needs between the combatant command and echelons above the combatant command (e.g., national agencies and Service intelligence centers); other command echelons supporting a combatant command; echelons below the combatant command (e.g., intelligence centers in corps, divisions, wings, and battle groups); multinational forces; and all tactical components. The mainline CIAP documents for each combatant command are the Command Intelligence Strategy Document, Command Intelligence Implementation Document, and Command Intelligence

Architecture Document. CIAP command unique documents include tactics, techniques and procedures (TTP) for intelligence support to joint operations, intelligence planning road maps, and subarchitectures for various intelligence functions and disciplines.

2. Deliberate Planning

Intelligence planners support the deliberate planning process which prepares for a possible contingency based on the best available information. Conducted primarily in peacetime, the deliberate planning process engages the entire joint planning community in the methodical development of plans for all contingencies and the transition to and from war. Figure II-1 shows the five phases of deliberate planning.

a. During Phase I, **Initiation**, the Services provide information to the supported commands on available intelligence forces and supplies required to support the plan. The Services also keep the combatant commander informed on Service intelligence plans and programs.

b. Phase II, **Concept Development** involves development of the supported commander's concept of the operation, documented as the commander in chief's (CINC's) Strategic Concept. The intelligence staff supports the development of alternative courses of action (COAs) by collecting and analyzing already existing information to produce intelligence on the adversary, terrain, meteorological and oceanographic (METOC) and geographic features that affect friendly and adversary forces through the joint intelligence preparation of the battlespace (JIPB) process. The CINC's strategic concept is forwarded to the Chairman of the Joint Chiefs of Staff (CJCS) for review and approval.

c. The approved CINC's Strategic Concept provides the basis for plan development by the CINC's staff. In Phase III, **Plan Development**, intelligence staffs are responsible for developing the Intelligence Annex and appendices to the basic OPLAN. Intelligence staffs must also identify intelligence support force and sustainment requirements and identify intelligence shortfalls throughout the planning process for incorporation into the OPLAN. Intelligence assets must be included in the time-phased force and deployment list (TPFDL) to ensure proper movement of critical personnel and equipment. The J-2 must coordinate with the

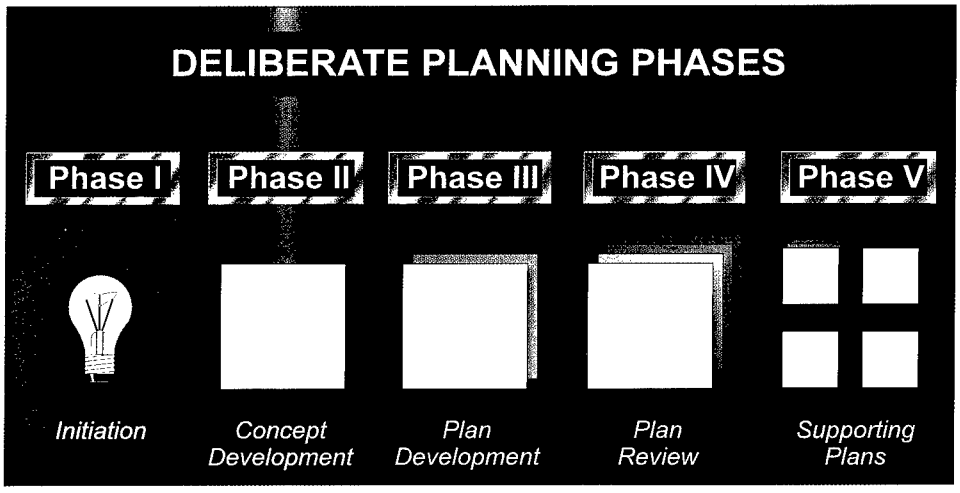


Figure II-1. Deliberate Planning Phases

combatant command J-6 to ensure intelligence communications requirements are incorporated in Annex K of the CINC OPLAN.

d. The Chairman of the Joint Chiefs of Staff conducts a final review of OPLANs submitted by the supported commander during Phase IV, **Plan Review**. This review evaluates the plan to determine whether taskings have been met and whether resources have been used effectively within the constraints of the Joint Strategic Capabilities Plan apportionment guidance. The Joint Staff J-2 reviews the intelligence annex for the Chairman. A sample intelligence annex is provided in Appendix D, "Intelligence Estimate."

e. Phase V, **Supporting Plans**, deals with mobilization, deployment, employment, sustainment, and redeployment of forces and resources in support of the concept described in the supported commander's approved plan. The Chairman of the Joint Chiefs of Staff may be asked to resolve critical issues, including use of intelligence forces and assets, that arise during the review of supporting plans. The Joint Staff may review any supporting plan on behalf of the Chairman.

3. Crisis Action Planning

a. The basic planning process is adapted to execute joint operations in crisis situations. **CAP procedures provide for the transition from planning military operations to actual execution through the timely flow of intelligence, rapid execution of military options, and the timely relay of decisions of the National Command Authorities (NCA) to supported commanders.**

b. Deliberate planning and CAP for any particular joint operation are interrelated by the degree to which deliberate planning has been able to anticipate and prepare for the crisis. Every crisis situation cannot be anticipated, but detailed analysis and coordination accomplished during the deliberate planning period may greatly expedite effective decision making and execution planning during crises and unanticipated contingencies. Therefore, joint intelligence support for CAP should always begin with a thorough exploitation of relevant deliberate plans.

c. **CAP and execution are accomplished within a framework of six phases** as described in Joint Pub 5-0, "Doctrine for Planning Joint Operations." Discussed below are the processes and procedures pertinent to joint intelligence planning during CAP.

- **Situation development** is a dynamic process that evolves simultaneously with policy. Proper situation development demands that staffs be able to provide immediate advice (within approximately 12 hours) to commanders based on deliberate planning. A principal task of the combatant command's J-2 is to help develop the commander's situation assessment. (Figure II-2) The intelligence effort focuses on intelligence collection and production to illuminate the situation for the combatant commander, components, subordinate JFCs, NCA, and Chairman of the Joint Chiefs of Staff. The command J-5, with the assistance of the J-2, reviews existing plans to determine if the particular event has been considered in deliberate planning. If an existing plan does not apply, the commander will need to develop priority intelligence requirements (PIRs) tailored to the mission early in the planning process to assess intelligence information gaps. Preliminary recommendations on the appropriate joint task force (JTF) composition should be considered at this point. The combatant command J-2 should notify the Defense Intelligence Agency (DIA), the National Security

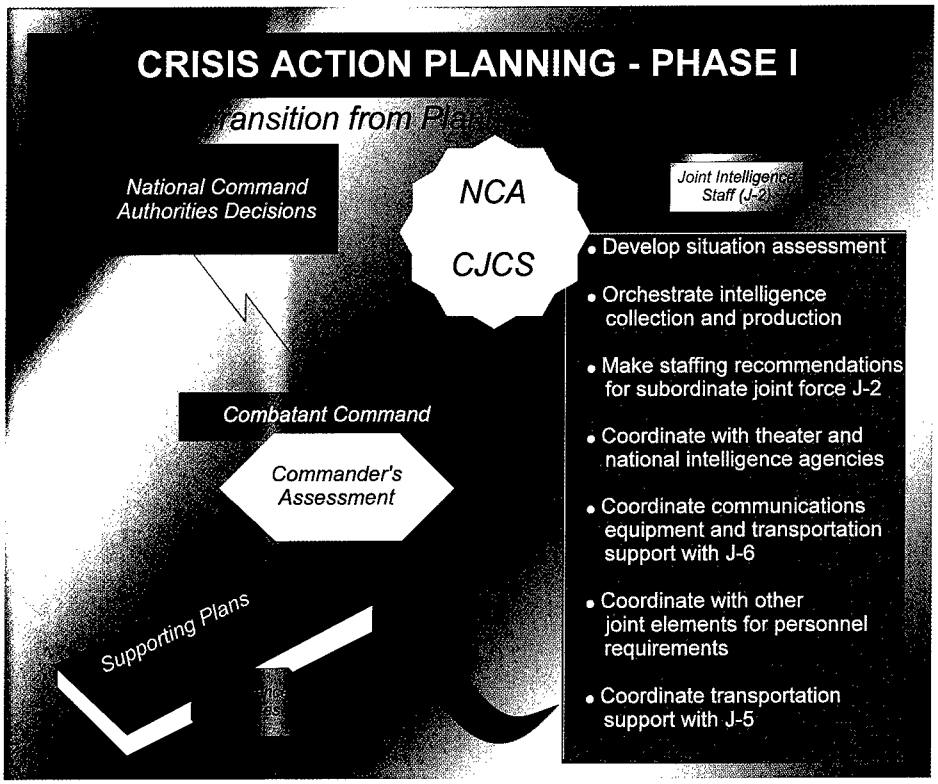


Figure II-2. Crisis Action Planning - Phase I

Agency (NSA), the Central Imagery Office (CIO), the Defense Mapping Agency (DMA), the Defense Information Systems Agency (DISA), the Joint Staff J-6, and any other relevant theater and national activities of requirements for intelligence, communications support, and manpower and equipment augmentation. The command J-2 should coordinate closely with the command J-3 and J-6 to ensure that these communications requirements receive sufficient priority in the command plan. Working with the command J-6, the command J-2 develops a subordinate joint force J-2 communications architecture that achieves interoperability laterally, vertically, and with multinational forces. It is also critical that intelligence planners work closely with their J-3, J-4, and J-6 counterparts to ensure priority for an early intelligence capability in support of deployed forces. Intelligence personnel, equipment, and communications paths must be part of the lead element in deployments to provide the commander with the best intelligence possible throughout the operation. The situation development phase ends when the CINC's assessment is submitted to the NCA and the Chairman of the Joint Chiefs of Staff.

- During Phase II, **crisis assessment**, the National Security Council (NSC), NCA, and the Chairman and other members of the Joint Chiefs of Staff analyze the situation assessment and determine whether a military option should be prepared. This phase requires increased intelligence gathering and analysis, particularly with respect to potential strategic lift destinations. Therefore, the

combatant command J-2 must work closely with national agencies to help define and then answer the emerging intelligence requirements of the senior leadership and answer the commander's PIR. (Figure II-3) The crisis assessment phase ends with a decision by the NCA to return to the pre-crisis state or to have military options developed for consideration and possible use. The NCA decision provides strategic guidance for joint operation planning and may include specific guidance on the COAs to be developed. The responsibilities of the theater J-2 during Phase II are as follows:

•• As required, the J-2 should nominate a subordinate joint force J-2 for consideration by the subordinate JFC. Once identified, the subordinate joint force J-2 then needs to coordinate with the combatant command J-2 and begin organizing, equipping, and preparing for the impending mission. Joint Pub 1-0, "Doctrine for Personnel Support to Joint Operations," provides doctrine on assigning personnel to meet combatant command and United Nations (UN) mission-related temporary duty assignments. Procedures include the combatant commander requesting intelligence personnel from the Joint Staff Manpower & Personnel Officer (J-1); the Director of Military Intelligence and the Military Intelligence Board validating and recommending resourcing of the requirement; and meeting crisis requirements by higher priority allocations for personnel fill. Reserves should be included in sustainment plans for long term joint force requirements such as Operation PROVIDE PROMISE.

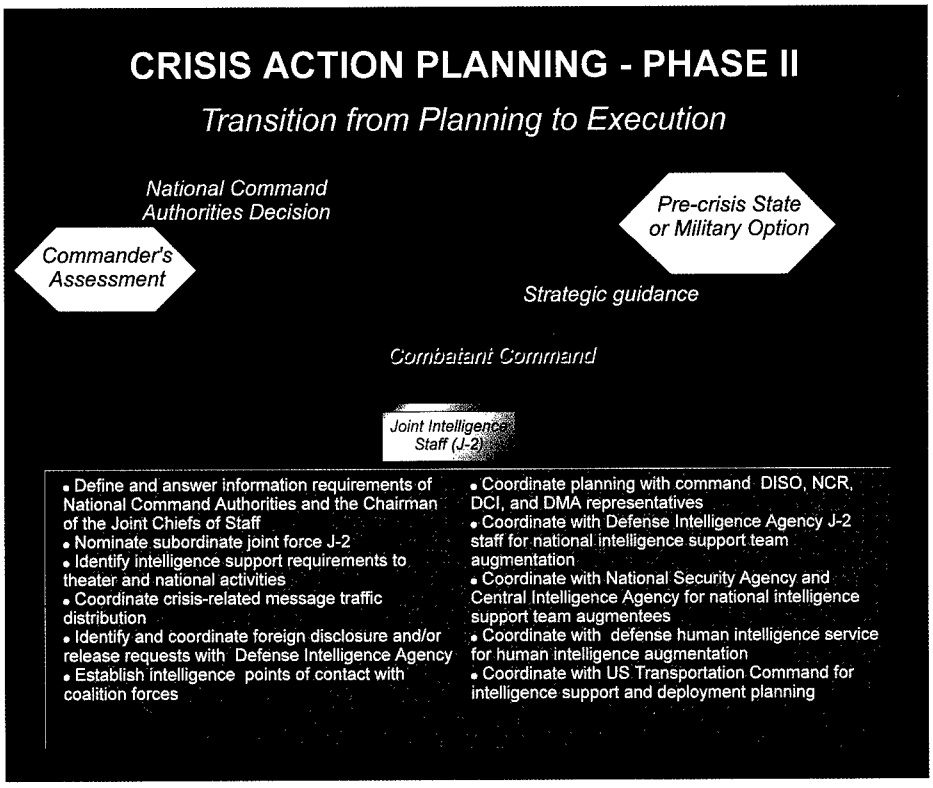


Figure II-3. Crisis Action Planning - Phase II

•• Coordinate with the combatant command Defense Intelligence Support Office (DISO), NSA and/or Central Security Service (CSS) Representative, Cryptologic Support Group (CSG), Director of Central Intelligence (DCI) representative, DMA and CIO representatives to ensure that they are informed of the NCA decision and the Chairman of the Joint Chiefs of Staff's planning guidance directive.

•• Coordinate with US Transportation Command (USTRANSCOM) J-2 and JIC to ensure that required intelligence is provided to transportation planners. Coordinate with the J-4 and J-5 to determine the effect that transportation infrastructure status has on deployment planning for intelligence assets as early as possible in the planning effort.

•• Coordinate with Joint Staff J-2 for National Intelligence Support Team (NIST) augmentation, if required. Be prepared to define NIST mission, the supported command, required team capabilities, number of teams required, geographic locations for deployment, and required deployment data.

•• Coordinate with the Defense Human Intelligence (HUMINT) Service (DHS) for HUMINT augmentation. The command HUMINT Support Element (HSE) is the conduit for this coordination.

•• Coordinate with the Counterintelligence Support Officer (CISO) for initiation of critical predeployment activities, realignment of ongoing CI support, and augmentation from the Services.

•• Notify all relevant theater and national activities of possible requirements for intelligence collection, production, processing, reporting, and/or dissemination assistance. Be prepared to state what assistance will be required, when it will be needed, and the duration of the requirement.

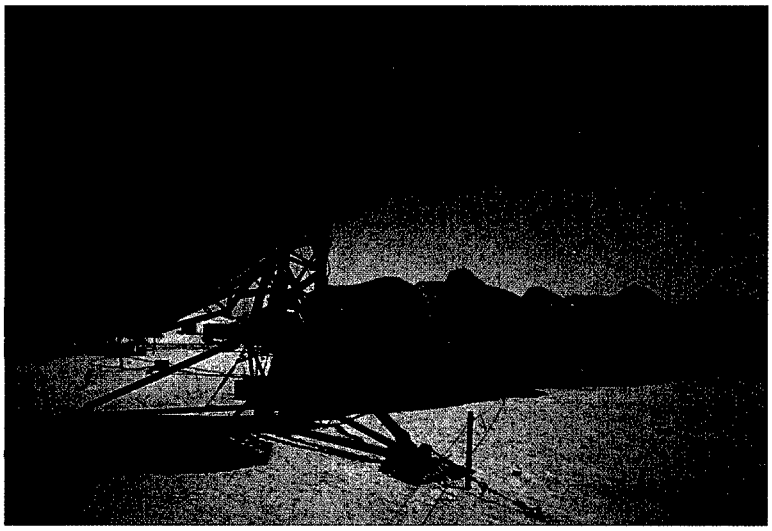
•• Implement and enforce procedures for requesting support from theater, Department of Defense (DOD) and non-DOD organizations, and any multinational forces. Identify problems and sensitivities. Requests for sensitive support will be coordinated with and processed through J-3 operations channels in accordance with (IAW) DOD Directive S-5210.36, "Provision of DOD Sensitive Support to DOD Components and Other Departments and Agencies of the US Government." All intelligence and other government agencies affected by or involved with sensitive support must also be kept informed.

•• Place the combatant command J-2 on distribution for all crisis-related traffic generated by theater and national intelligence activities. Ensure that the combatant command J-2 has access to any compartmented message traffic. Review the command's statements of intelligence interest (SIIs), which are key to receipt of intelligence traffic and special requests for documents. Coordinate changes with DIA.

•• Identify, in coordination with the J-3 and J-4, requirements and/or requests from foreign countries for assistance or information. If required, begin coordinating requests for foreign disclosure and/or release with DIA. Consult with the Joint Staff J-2 on the status of possible UN actions and associated intelligence support requirements.

•• Establish points of contact with coalition forces. Determine if any special language or translation requirements exist which will necessitate linguist augmentation.

•• Coordinate with US Space Command (USSPACECOM) for Joint Space Support Team (JSST) augmentation. USSPACECOM will deploy task-organized JSSTs to the supported command to provide space-derived intelligence, and ensure that support is provided. Information required includes: specific support teams, where they will be located, what is required, and approximately when the teams are required to be in place.



The sequenced arrival of J-2 personnel and equipment, including NIST assets, needs to be planned and coordinated early.

•• Coordinate with the Joint Command and Control Warfare Center (JC2WC) for augmentation and intelligence support to IW and/or command and control warfare (C2W).

- Phase III, **COA development**, begins with a CJCS Warning Order activating the designated JTF. It implements an NCA decision or CJCS planning directive to develop military options. This directive and required actions are described in Joint Pub 5-0, "Doctrine for Planning Joint Operations," and Joint Pub 5-00.2, "Joint Task Force Planning Guidance And Procedures." The supported commander analyzes each COA and provides recommendations to the NCA and Chairman of the Joint Chiefs of Staff. Figure II-4) This phase ends with submission of the supported commander's estimate, which includes the intelligence estimate (Appendix D).

•• To this point, planning for subordinate joint force J-2 operations has been centered in the combatant (supported) command J-2. During Phase III, the subordinate joint force J-2 staff begins forming a JISE and assumes leadership for J-2 CAP. A JISE will provide the JFC with complete intelligence on the air, space, ground, and maritime adversary situation.

•• Subordinate joint force J-2 mobility considerations include the following:

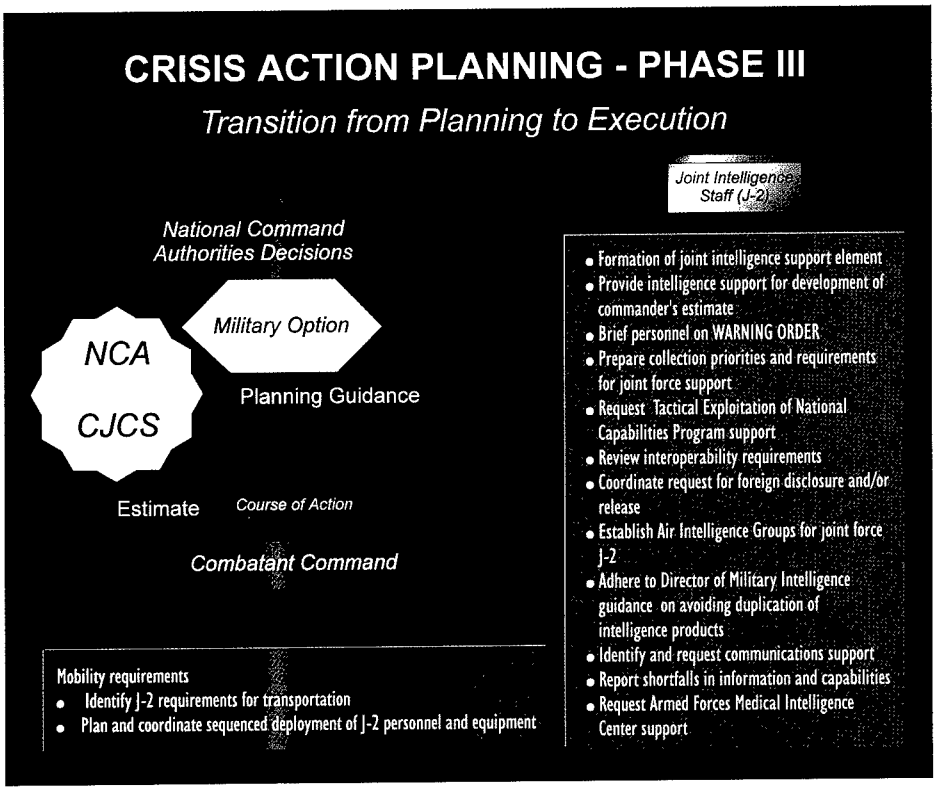


Figure II-4. Crisis Action Planning - Phase III

(1) The supported command forms a subordinate joint force, with planning centering on the issues of mobilization and sustainability for the joint force. J-2 requirements for transportation are entered into JOPES during this phase. Input must include anticipated requirements for attachments such as NIST and augmentation to HUMINT Operations Cell (HOC) and to the Task Force Counterintelligence Coordinating Authority (TFCICA). (2) The subordinate joint force J-2 should keep JOPES managers up-to-date on intelligence personnel and equipment movement requirements. The sequenced arrival of deployed J-2 personnel and materiel, including NIST assets, needs to be planned and coordinated early. Points of contact (POCs) should be identified to work with the combatant command J-3 and/or J-4 as well as joint force J-3 and/or J-4 on J-2 movement requirements. Requesting commands must logistically support the NIST and other external augmentation elements. If required, formal requests must be submitted for support from CIO and DISA. DISA requests must be coordinated with the J-6.

•• Key planning actions of the combatant command J-2 in coordination with or as requested by subordinate JTF J-2, are as follows: (1) Ensure that the supported commander receives all the intelligence support needed from the command J-2 to develop the COA for the commander's estimate. (2) Brief the subordinate joint force J-2 personnel on mission objectives and guidance contained in the warning order. Ensure that all members of the subordinate joint force

J-2 staff review theater TTP, Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations," and Joint Pub 2-02, "National Intelligence Support to Joint Operations," and understand their responsibilities and required actions. (3) Evaluate systems, supply, and equipment requirements associated with each COA. Mobility planning requires a decision on what to ship to the subordinate joint force location in what priority. Identify external theater and/or national intelligence and communications systems required to support subordinate joint force operations. Include this information in the commander's estimate. (4) Brief combatant command J-2 staff on the warning order. If appropriate, advise them of potential requirements for augmentation (personnel and/or equipment). Based upon subordinate joint force J-2 stated requirements, the joint force J-1 will resource additional personnel through the combatant command J-1. (5) Prepare general collection priorities and requirements for subordinate joint force support and coordinate requirements with the combatant command J-2. The combatant command J-2 coordinates with national collection authorities at DIA, NSA, CIO, DMA and the Central Intelligence Agency (CIA) to notify them of impending requirements and determine availability of resources. (6) If required, request Tactical Exploitation of National Capabilities (TENCAP) support. The J-2 can request additional TENCAP support, including prototype and demonstration systems, through Service TENCAP offices. (7) Review facility security requirements. Prepare request(s) for accreditation of facilities, if required. (8) Continue to review requirements for systems interoperability and/or interconnectivity, and report on possible multi-Service and/or multinational interoperability problems. Coordinate with the agencies and organizations involved. (9) Continue to coordinate requests for foreign disclosure and/or release issues with DIA, as appropriate. Obtain waivers if required. (10) Establish new addressee indicator group (AIG) for receiving and sending pertinent subordinate joint force J-2 message traffic. Arrange to put the subordinate joint force J-2 on distribution for message traffic, intelligence products, and reports. Review and adhere to policies on assigning precedence to intelligence messages, especially for summaries. (11) Eliminate duplicative intelligence and avoid unnecessary redundancy in the re-transmittal or rebroadcast of intelligence information. (12) Identify combatant command, Service, or subordinate joint force J-2 requirements for communications support. Coordinate all requirements for systems and frequencies with the combatant command and subordinate joint force J-6. Forward requests for national-level communications support through the combatant command J-6 to the Joint Staff J-2 for validation and the Joint Staff J-6 for tasking. (13) Coordinate a Joint Restricted Frequency List with the command J-2, J-6, and NSA. (14) Report major capability limiting factors (shortfalls) in any area for possible inclusion in the commander's estimate. (15) Request a current profile on disease and environmental hazards from the DIA Armed Forces Medical Intelligence Center.

•• Review the checklist found in Joint Pub 5-00.2, "Joint Task Force Planning Guidance and Procedures," Appendix C, Annex B. This checklist covers the questions that the J-2 must consider for the subordinate joint force OPORD.

- Two critical events highlight Phase IV, **COA selection**: selection of a COA by

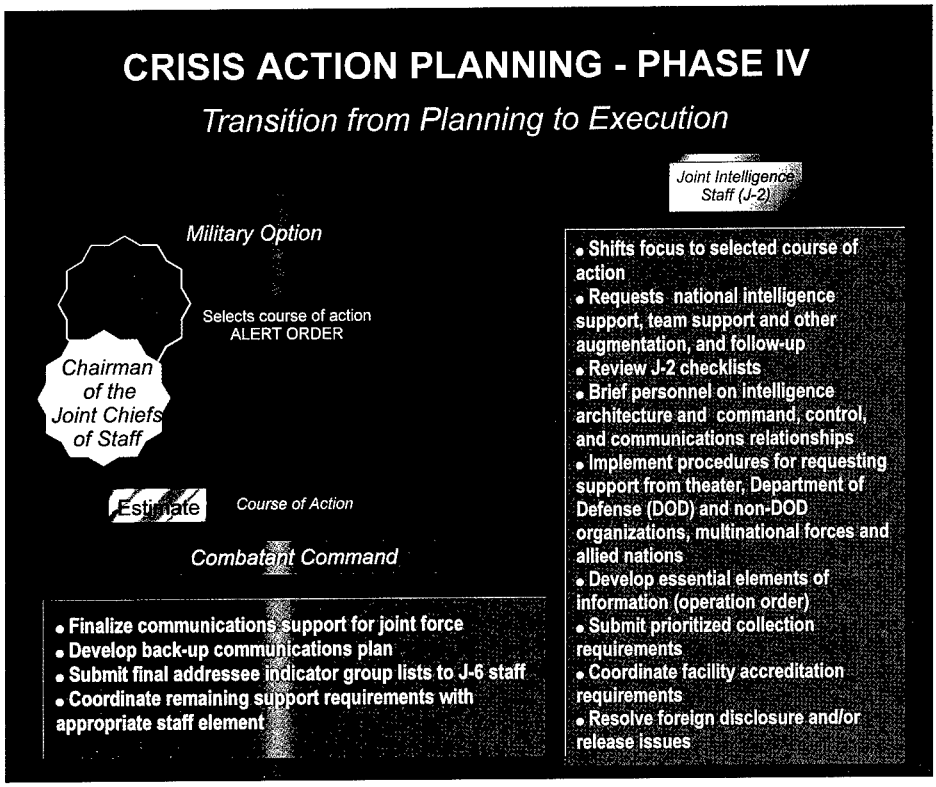


Figure II-5. Crisis Action Planning - Phase IV

the NCA and initiation of execution planning. (Figure II-5) The Chairman of the Joint Chiefs of Staff reviews and evaluates the combatant commander's estimate and prepares recommendations and advice for the NCA. The NCA selects a COA and directs that execution planning be accomplished. An alert order implements the NCA decision and contains sufficient detail to allow the JFC to conduct detailed planning. A CJCS planning order could be issued to initiate execution planning before the NCA selects a COA. The subordinate joint force J-2 planning action focus shifts to the COA selected by the NCA. In addition, the subordinate joint force J-2 will act as follows:

•• Coordinate with Joint Staff J-2 for NIST and other augmentation from national intelligence agencies (DIA, NSA, CIO, and/or CIA). Submit all support requests to Joint Staff J-2 via the combatant commander for validation and subsequent action. Follow-up on any requests submitted earlier in the planning process.

•• Ensure that all subordinate joint force J-2 personnel understand the organizational structures, command, support and multinational relationships established for the mission. Joint force J-2 personnel should be briefed on key command and control relationships affecting their specific responsibilities.

•• Finalize communications support for the subordinate joint force J-2. Develop back-up procedures, in coordination with the J-6, for maintaining support to customers if primary communications are lost.

•• Prepare and publish the PIR pertinent to the upcoming mission. PIR are formally published in the OPORD during Phase V.

•• Publish and distribute the concept of operations for the subordinate joint force JISE. The JISE evolves and is sized to meet the specific crisis or contingency with an intelligence structure that matches the mission.

•• Submit AIGs to J-6 for sending and receiving message traffic.

•• Ensure that requests for theater and national augmentation (personnel and equipment) are formally submitted and track response. Coordinate with J-1 to ensure that logistical preparations for locating and housing augmentees are underway.

•• Coordinate final personnel, systems, supply, equipment and communications security materials requirements with subordinate joint force J-1, J-3, J-4, J-5, and J-6, and submit them per command procedures for inclusion in JOPES and the TPFDD.

•• Submit prioritized collection requirements for validation by theater and national authorities. Inform combatant command reconnaissance planners and schedulers of required start date for theater-based reconnaissance support.

•• Submit and track the request for facility accreditation to ensure that a decision is made.

•• Resolve foreign disclosure and/or release procedures. Inform all subordinate joint force personnel of procedures for handling disclosure and/or release of intelligence to foreign nationals. Requirements and procedures for sharing intelligence with multinational forces must be finalized and specific products to be shared must be identified in the JISE concept of operations and in the OPORD. Coordinate with the Joint Staff J-2 for support being provided to multinational forces through the UN, North Atlantic Treaty Organization (NATO), or other international organizations.

- Phase V, **Execution Planning**, begins with receipt of the alert order or planning order from the Chairman of the Joint Chiefs of Staff. The approved COA is transformed into an OPORD. Detailed planning occurs throughout the joint planning community. If required, the supported commander will initiate campaign planning or refine a campaign plan already developed. The supported commander develops the OPORD and supporting TPFDD by modifying an existing OPLAN, expanding an existing CONPLAN, or developing a new plan. (Figure II-6) This phase ends with an NCA decision to implement the OPORD. In those instances where the crisis does not progress to implementation, the Chairman of the Joint Chiefs of Staff provides guidance on continued planning using either deliberate or CAP procedures.

•• The planning emphasis during this phase shifts to transportation requirements and the building of movement schedules. The supported commander and subordinate joint force J-2 track these developments closely. The status of J-2 movement requirements should be included in every status report and briefing prepared during the planning of joint force operations.

•• Appropriate subordinate joint force J-2 planning actions during this phase

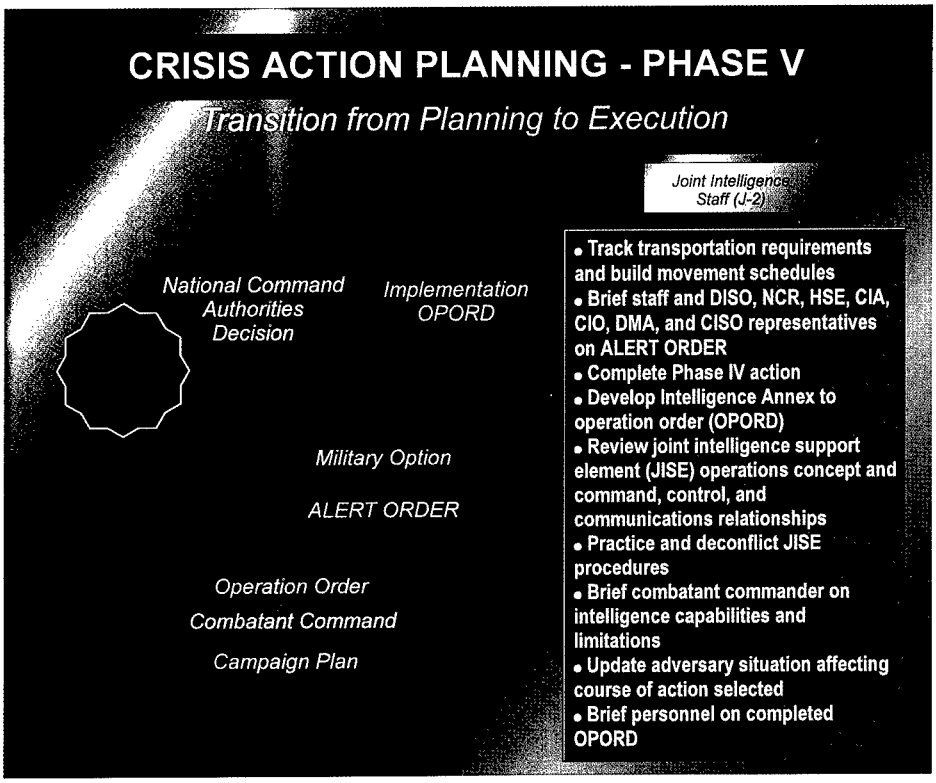


Figure II-6. Crisis Action Planning - Phase V

THEATER INTELLIGENCE

The primary focus of intelligence operations, particularly during Operation DESERT SHIELD, was to provide the theater and component commanders with an accurate picture of Iraqi capabilities and intentions. To do so, the theater-level intelligence structure made extensive use of national capabilities as well as a wide array of deployed Service and component capabilities. In some cases, collection platforms and systems organic to tactical units were tasked for missions that did not directly support their parent organizations. Although some shortfalls surfaced, theater-level intelligence efforts met the requirements of CINCCENT and his component commanders.

SOURCE: Final Report to Congress Conduct of the Persian Gulf War, April 1992

include the following: (1) Brief the subordinate joint force J-2 staff, DISO, National Security Agency/Central Security Service Representative (NCR), CSG, HSE, CISO, CIO, DMA, and CIA representatives on the alert or planning order. (2) Finalize any remaining Phase IV or previous actions that were compressed due to fast-paced development of the crisis situation. (3) Review Appendix C in Joint Pub 5-00.2, "Joint Task Force Planning Guidance and Procedures," and Appendix B of this publication, "Representative

Intelligence Requirements," which list general intelligence responsibilities associated with a subordinate joint force. Develop the OPORD's Annex B (Intelligence) according to CJCSM 3122.04, "Joint Operation Planning and Execution System, Vol II: (Supplemental Planning and Execution Formats and Guidance)." (4) Ensure that all personnel have reviewed and understand the JISE operations concept. Ensure that C4 systems relationships have been defined for support to major component forces of the subordinate joint force. (5) Ensure that JISE procedures affecting highly time-sensitive and mission-critical operations and/or intelligence interfaces are thoroughly practiced and deconflicted. Highly time-sensitive interfaces usually include special operations forces (SOF) operations, targeting, and the Joint Search and Rescue Center. Other interfaces may be created depending upon how the subordinate joint force is constituted. Requests for SOF and other specialized time-sensitive operational support will be coordinated through J-3 operations and may require special category communications procedures. (6) Apprise the supported commander of the current status of intelligence capabilities and limitations. (7) Enumerate changes, if any, in the adversary's situation that could require a change in the COA selected. (8) Brief subordinate joint force J-2 personnel on the completed OPORD.

- If the NCA decide to execute the selected COA, the Chairman of the Joint Chiefs of Staff issues an execute order during Phase VI, **Execution**. The execute order directs the employment and deployment of forces, defines the timing for initiation of operations, and conveys guidance not provided in earlier CAP orders and instructions. This phase continues until the crisis or mission ends and force redeployment has been completed. If the crisis is prolonged, the process may be repeated continuously as circumstances change and missions are revised. If the crisis expands to major conflict or war, CAP will evolve into and be absorbed within the larger context of implementation planning for the conduct of the war. The subordinate joint force J-2 provides intelligence critical to current and future operations, planning, targeting, and force protection. Collection, analysis and reporting must answer the commander's PIR and provide predictive intelligence and assessments, with emphasis on intelligence involving the movement and disposition of hostile forces. Adversary movements of interest to SOF are among the top joint force reporting priorities throughout Phase VI. The supported command J-2 must be prepared to assume this reporting responsibility until the subordinate joint force J-2 has reached operational status at the deployed location. (Figure II-7)

4. Campaign Planning

The theater campaign plan embodies the combatant commander's vision of related major operations required to attain strategic objectives. Campaign planning is appropriate **when military operations exceed the scope of a single major operation.** It encompasses both the deliberate and CAP processes. Intelligence supports all aspects of the campaign plan. (Figure II-8)

a. A campaign is a series of related military operations aimed to achieve strategic and operational objectives. **A campaign plan describes how a series of these operations is arranged in time, space and purpose.** The plan focuses on the adversary's centers of gravity; simultaneous and synchronized employment of land, sea, air, space-based, and SOF assets; and the end state to be achieved.

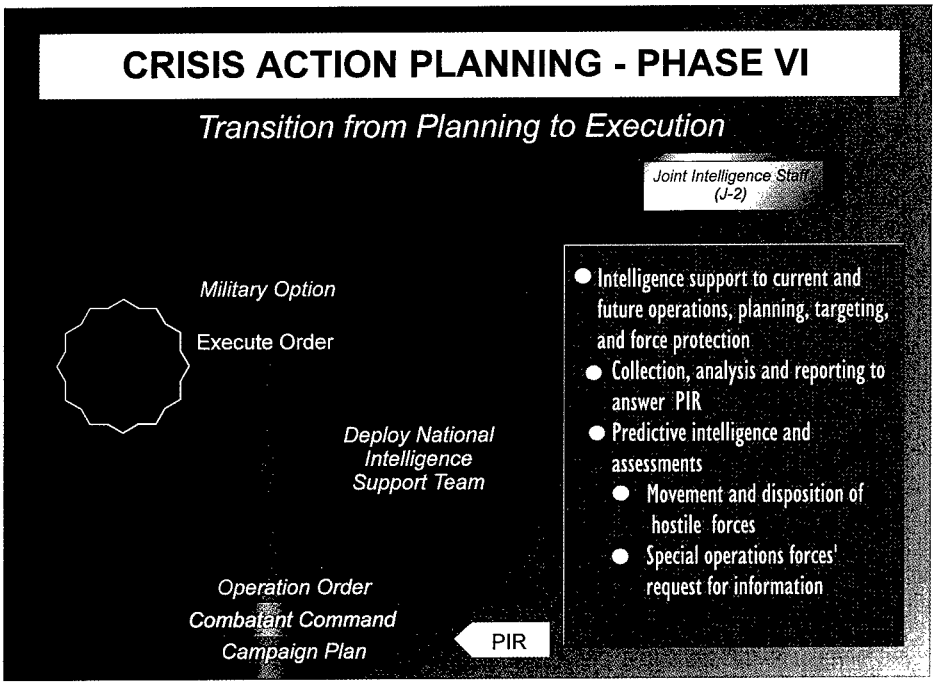


Figure II-7. Crisis Action Planning - Phase VI

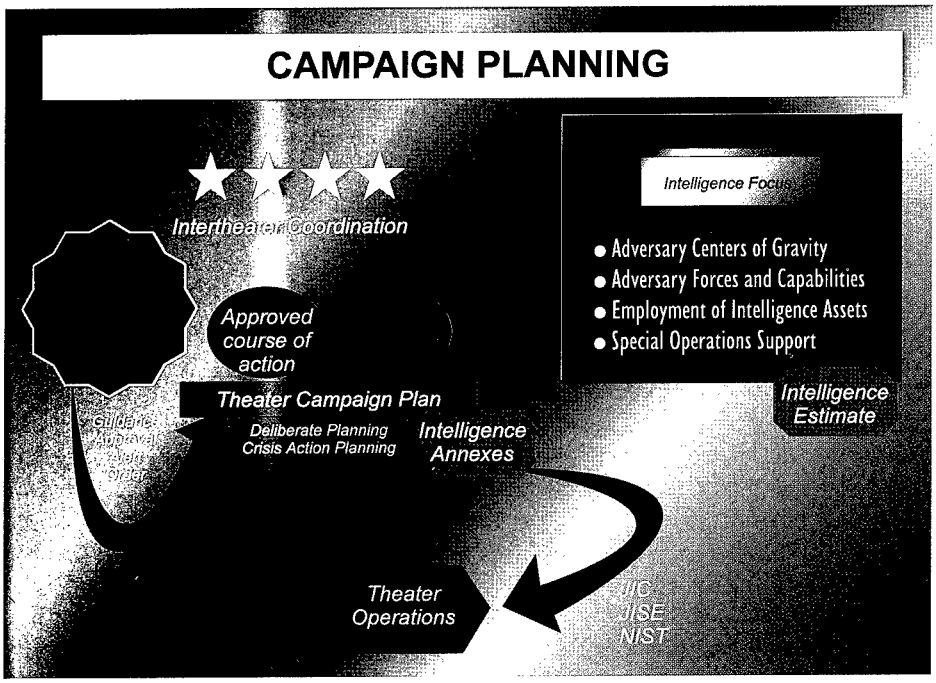


Figure II-8. Campaign Planning

It serves as the basis for subordinate planning. A campaign plan provides the NCA and the Chairman of the Joint Chiefs of Staff with the information needed for intertheater coordination at the national level.

b. Campaign plans guide the development of supporting OPLANs and OPORDs. COAs are developed and forwarded in the commander's estimate for approval by the NCA. The combatant commander finalizes the campaign plan based on a CJCS alert order, using the approved COA as the centerpiece. Intelligence efforts in support of the campaign plan, including the intelligence annexes, focus on identifying any adversary forces and capabilities in the area of responsibility (AOR) and/or the joint operations area (JOA) and the adversary's strategic and operational centers of gravity.

5. Multinational Operations

There is a strong likelihood that military operations will take place under bilateral, multinational, or UN auspices. Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations," discusses intelligence support for multinational operations and describes the intelligence principles that guide the JFC and J-2 in organizing and sharing intelligence with multinational forces.

6. Conclusion

The time required to plan subordinate joint force J-2 support depends largely upon how much can be adapted from already existing deliberate plans and the total time required for the CAP process in a given situation. In some cases, events could cause planning to skip directly to the execution phase. To prepare for this eventuality, combatant command J-2s should create their own crisis planning checklists and exercise them. Appendix A, "Joint Force J-2 Quick Reaction Checklist," provides a starting point for checklist development.

Intentionally Blank

CHAPTER III
THE INTELLIGENCE CYCLE

"... that no war can be conducted successfully without early and good intelligence, and that such advices cannot be had but at very great expense."

The Duke of Marlborough 1650-1722

1. Introduction

a. Intelligence operations follow the intelligence cycle. **The intelligence cycle focuses on the commander's mission and concept of operation.** Intelligence operations have to be integrated into overall joint operations to achieve the JFC's objectives.

b. The intelligence cycle conceptual model describes the process used to produce intelligence. There are no firm boundaries delineating where each phase of the cycle begins or ends. The intelligence cycle provides a process to understand and order the many activities involved in intelligence and is useful for understanding the interrelationships of the intelligence phases. The intelligence process may not continue through the entire cycle. For example, during the processing and exploitation phase data may be passed directly to the user from an unmanned aerial vehicle (UAV) or other source, instead of being processed or exploited first.

c. **Activities during each phase of the intelligence cycle (Planning and Direction, Collection, Processing and Exploitation, Production, Dissemination and Integration, and Evaluation) directly support the JFC.** (Figure III-1) The JFC depends on timely, accurate intelligence on an adversary's strategy, tactics, intent, objectives, strengths, weaknesses, values, and critical vulnerabilities.

d. Joint intelligence operations begin with a need for intelligence regarding the adversary or environment in the AOR/JOA. The J-2, in coordination with other staff elements, develops proposed PIR early in the deliberate planning process. PIR are those critical pieces of intelligence that the commander must know about the opponent and the operational environment by a particular time in order to plan and execute a successful mission. PIR are identified at every level, from tactical to national, and are drafted for the commander's approval by the intelligence staff. PIR are based on guidance obtained from the commander's mission statement, the OPLAN objectives, and the commander's intent.

2. An Overview

a. The intelligence requirement provides the direction for current and future intelligence operations during the **Planning and Direction** phase, where the requirement is prioritized by the collection requirements management (CRM) staff. The combatant command and/or the subordinate joint force J-2 provides the focus and direction for collection requirements to support the combatant command or subordinate joint force.

b. The next phase, **Collection**, involves tasking appropriate collection assets and/or resources through the collection operations management (COM) staff to acquire intelligence information to satisfy collection objectives. Collection includes the identification and positioning of assets and/or resources to satisfy collection objectives.

c. Once the data that might satisfy the requirement is collected, the intelligence process enters the **Processing and**

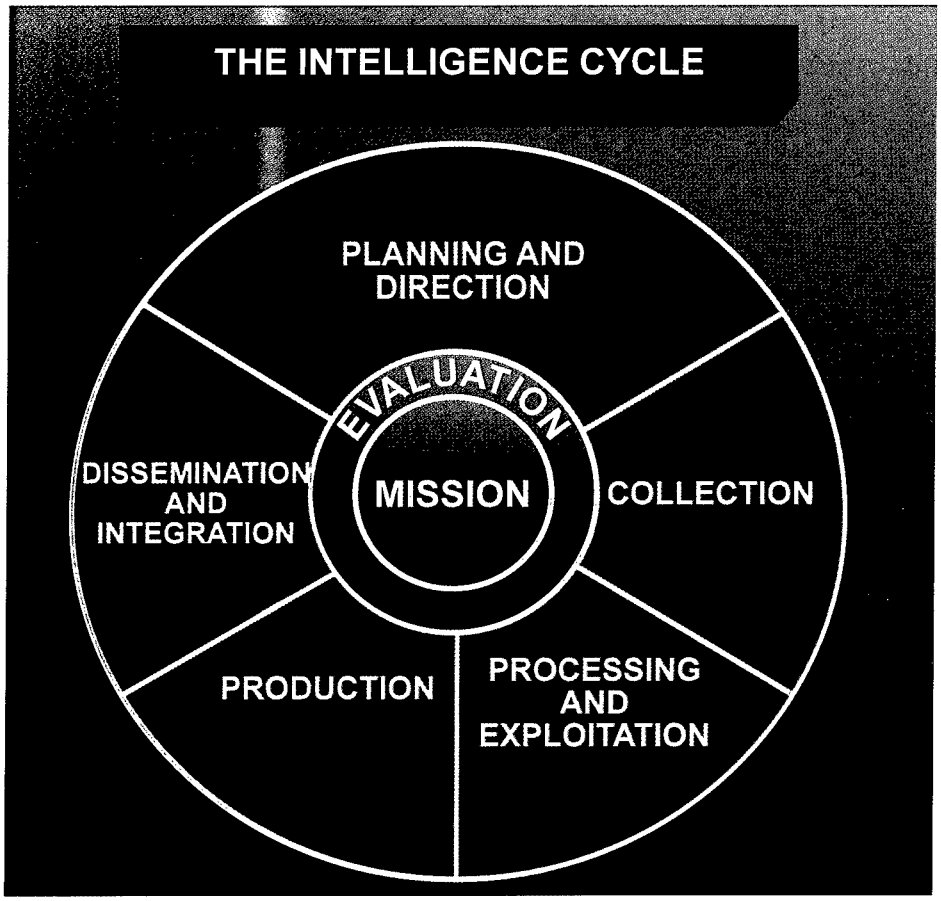


Figure III-1. The Intelligence Cycle

Exploitation phase. The collected data is exploited and transformed into a product that can be readily used in the analysis and production of intelligence. Processing and exploitation must be prioritized and synchronized with the commander's PIR.

d. The **Production** phase involves integrating, evaluating, analyzing, and interpreting information from single or multiple sources into a finished intelligence product. Time constraints and demands of the modern battle tend to make the processing and production phases indistinguishable.

e. A product enters the **Dissemination and Integration** phase of the intelligence cycle and is formatted to meet the requirement. The product is disseminated to the requester, who integrates the intelligence into decision making and planning processes.

f. Intelligence personnel at all levels **Evaluate** how well the intelligence phases work throughout the intelligence cycle.

g. If the intelligence provided to the requester is complete, timely, and in a usable format, the requirement is satisfied and subsequently closed. A requirement is not satisfied when resulting intelligence does not meet the above criteria; if time permits, the requirement can be retasked. When a satisfied requirement results in a new request, a new requirement is generated and the process is repeated.

3. The Intelligence Cycle and Joint Operations

Intelligence supports joint operations, focusing on providing multidiscipline intelligence support to the combatant command, the subordinate Service and functional component commands, and subordinate joint forces. The remainder of this chapter discusses each phase of the cycle in detail (the evaluation process is addressed under each phase) and describes the intelligence activities that occur in each phase. Intelligence cycle execution responsibilities are depicted in Appendix H, "Intelligence Cycle Execution Responsibilities."

SECTION A. PLANNING AND DIRECTION

4. Overview

The first phase of the intelligence cycle is planning and direction. **While conducted continuously, intelligence planning and direction normally occurs during and in conjunction with operation planning.** JIPB helps the joint force J-2 focus and direct this phase and the remaining phases of the intelligence cycle. **Planning and directing involves the activities shown in Figure III-2.**

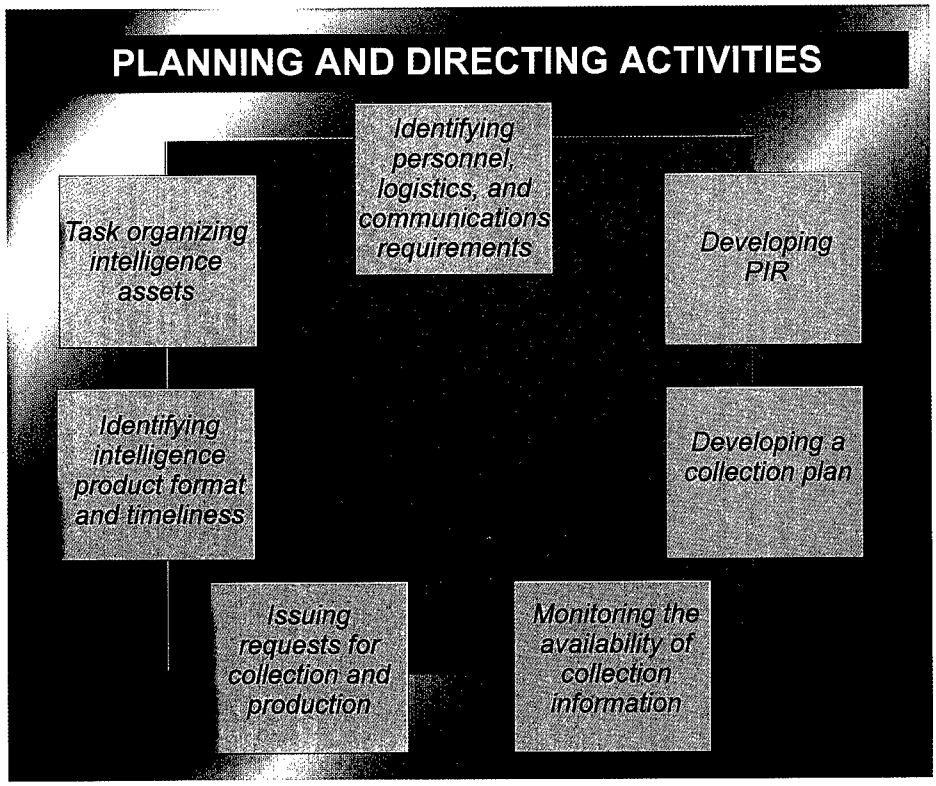


Figure III-2. Planning and Directing Activities

5. Organizations and Responsibilities

The supported combatant commander establishes command relationships among all elements made available to the joint operation. Sharing and mutual support are essential to integrating all resources and capabilities into a unified system that will best fulfill the prioritized intelligence needs for joint operations.

a. **National-Level Intelligence Organizations.** The DIA J-2 NMJIC is the focal point for intelligence activities in support of joint operations. **Joint force intelligence requirements are forwarded through the combatant command JIC to the NMJIC where appropriate national assets are tasked.** Joint Pub 2-02, "National Intelligence Support to Joint Operations," details the structure of national-level support to joint operations and describes the functions of national-level entities and the NMJIC. National-level agencies include DIA, NSA, CIA, the National Reconnaissance Office (NRO), the Defense Airborne Reconnaissance Office, CIO, DMA, the Department of State, and the national-level intelligence elements of the military Services.

b. **Unified Command.** The unified command's JIC is organized IAW combatant commander prerogatives, but normally performs the general functions described in Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations," and specific unified command intelligence TTPs. **The responsibility for providing intelligence support to military operations rests with the JIC.** If the JIC cannot meet the combatant commander's requirements, the JIC forwards requests to the NMJIC or to subordinate command levels through established channels, using standard command procedures. In some cases, the JIC may also seek to ensure timely support by approving in advance a direct communication path between requesters and outside producers, so long as the JIC is informed of all requests as they are made. This method is most appropriate when operators require products and services that are not routinely produced by the JIC.

c. **Subordinate Joint Force**

- Within the context of a geographic combatant command, **individual subordinate joint force J-2 organizational structures will be situation and mission-dependent, as determined by the JFC.** All subordinate joint force J-2s, however, will at a minimum require a core element of analytical and administrative capabilities. Joint Pub 1-0, "Doctrine for Personnel Support to Joint Operations," governs the use of intelligence personnel assigned to meet combatant command and UN mission-related duty requirements.

- The subordinate joint force J-2 provides administrative support to augmentation forces and the JISE, including personnel, information, and physical security. **Capabilities of the JISE include order of battle (OB) analysis, identification of adversary centers of gravity, analysis of C4, targeting support, collection management, and maintenance of a 24-hour watch.** In coordination with the theater J-2, a joint force J-2 counterintelligence and/or human intelligence staff element (J-2X) may also be activated. This concept is designed to integrate HUMINT and CI by combining the HOC with the TFCICA, both of whom comprise the J-2X. The J-2X is responsible for controlling and coordinating all HUMINT and CI collection activities and keeping the joint force J-2 informed on all HUMINT and CI activities conducted in the joint force AOR.

- In addition to declared hostilities, **MOOTW may require the deployment**

and assistance of theater intelligence elements to include humanitarian aid missions, disaster relief operations, counterdrug actions, and terrorist and hostage events. In every case, the concept of preplanned, dedicated joint force J-2 intelligence support (NIST, DHS, or other joint force J-2 intelligence support) keyed to a wide variety of theater support options provides a sound foundation to respond to crisis requirements.

- An example of a possible subordinate joint force J-2 organizational support package is shown in Figure III-3. This hypothetical structure should only be used as a point of departure when planning and organizing a subordinate joint force JISE. The nature and magnitude of the crisis will dictate the actual size and configuration of the JISE.

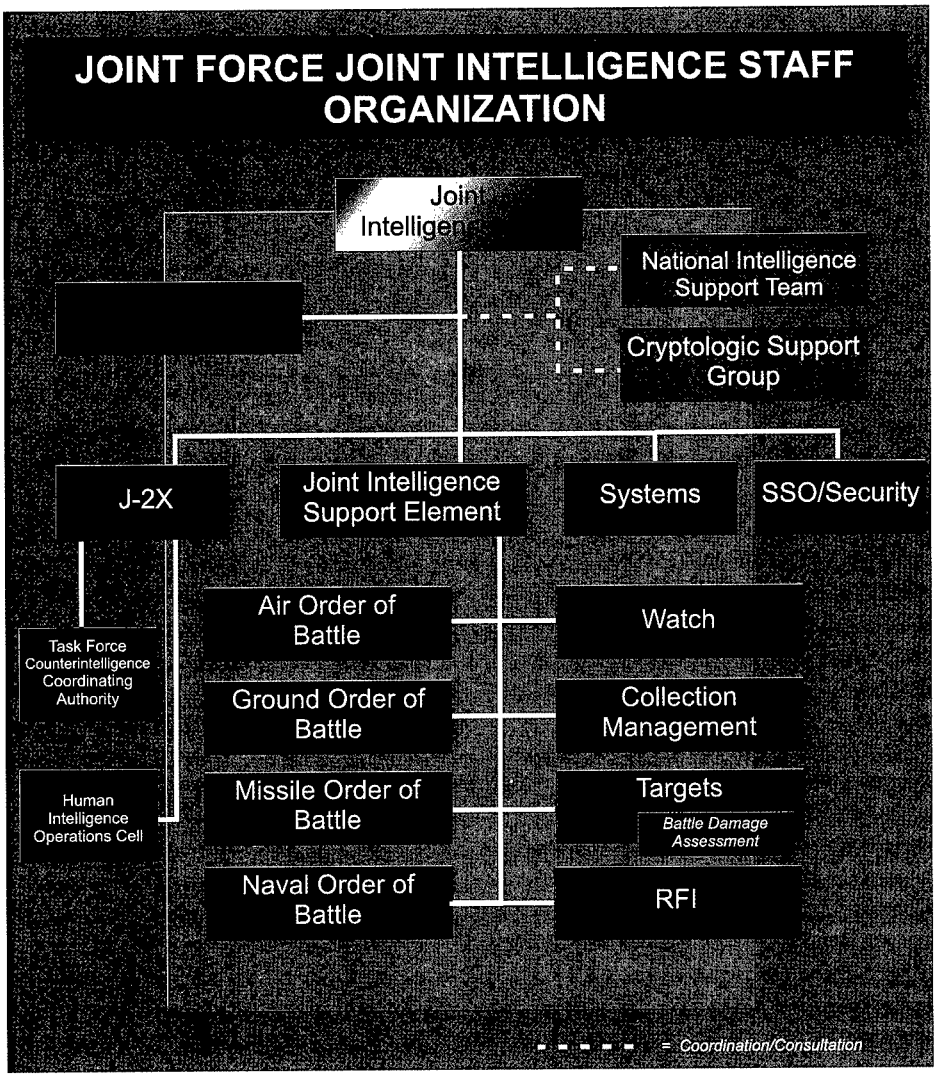


Figure III-3. Joint Force Joint Intelligence Staff Organization

6. Augmentation Requirements

a. Optimum use of available intelligence assets is essential to ensure quality support in meeting the proliferation of customer requirements. **The demand for additional intelligence support increases significantly during crisis and wartime operations.** Not only are more intelligence personnel needed in the AOR and/or JOA, but the intelligence presence increases at all command levels. Locating additional personnel and knowing how to obtain their services is vital. Personnel augmentation requirements should be in accordance with CJCS Instruction 1301.01, "Policy and Procedures to Assign Individuals to Meet Combatant Command Mission Related Temporary Duty Requirements," and reflected in the combatant command's joint table of mobilization and distribution (JTMD). The JTMD should reflect the need for either individual mobilization augmentees (IMAs) or individual ready reserve (IRR) personnel. An IMA is preassigned, trains annually at the same activity to which assigned in a contingency, and requires knowledge of the intelligence mission. An IRR augmentee does not require an in-depth knowledge of the combatant command's intelligence mission, and may have never trained or been assigned to an intelligence organization. When an operation is anticipated or commences, personnel requirements should be refined and requests initiated. Reserve personnel requirements can usually be identified in advance by exercising the OPLAN or the intelligence portion of the OPLAN.

b. In a crisis, the JFC states the requirements, including personnel needed to support military operations. The supported command, through its Service components, takes the lead in augmenting its staff and the joint force. The Joint Staff takes the lead in augmenting the NMJIC intelligence staff. Augmentation requirements are depicted in Figure III-4.

- Normally, **active duty intelligence personnel are reassigned to support the operation on a temporary basis** within-theater through established personnel management channels.

- On a national level, the NCA can direct active duty assets to new assignments in support of the joint force. **Additionally, teams of intelligence personnel can be positioned for crisis deployment (NIST, HOC, or other teams of intelligence personnel) upon receipt of a requirement from the supported combatant command**. Each of the Services and intelligence community agencies have established channels to deploy mission-specific intelligence teams and support personnel. Requesting commands must be prepared to support logistically the NIST and other external augmentation elements.

- During a national emergency or a response to lower-level requirements, **reserve intelligence individuals or units may be called to active duty**. Reserve units and individuals in all four Services are trained and experienced in a number of key duties, such as collection management, dissemination management, imagery intelligence (IMINT) and signals intelligence (SIGINT) analysis, languages, and CI. Reservists may serve at any time on voluntary active duty orders or may be ordered involuntarily to active duty under either a Presidential Selected Reserve Callup or partial or full mobilization. The extent and period of reserve augmentation depends on requirements and funding availability.

c. **A combatant command may make a request to the NMJIC for specific national intelligence agency capabilities.** The NMJIC will evaluate and coordinate combatant command requirements with the J-3/J-5 and

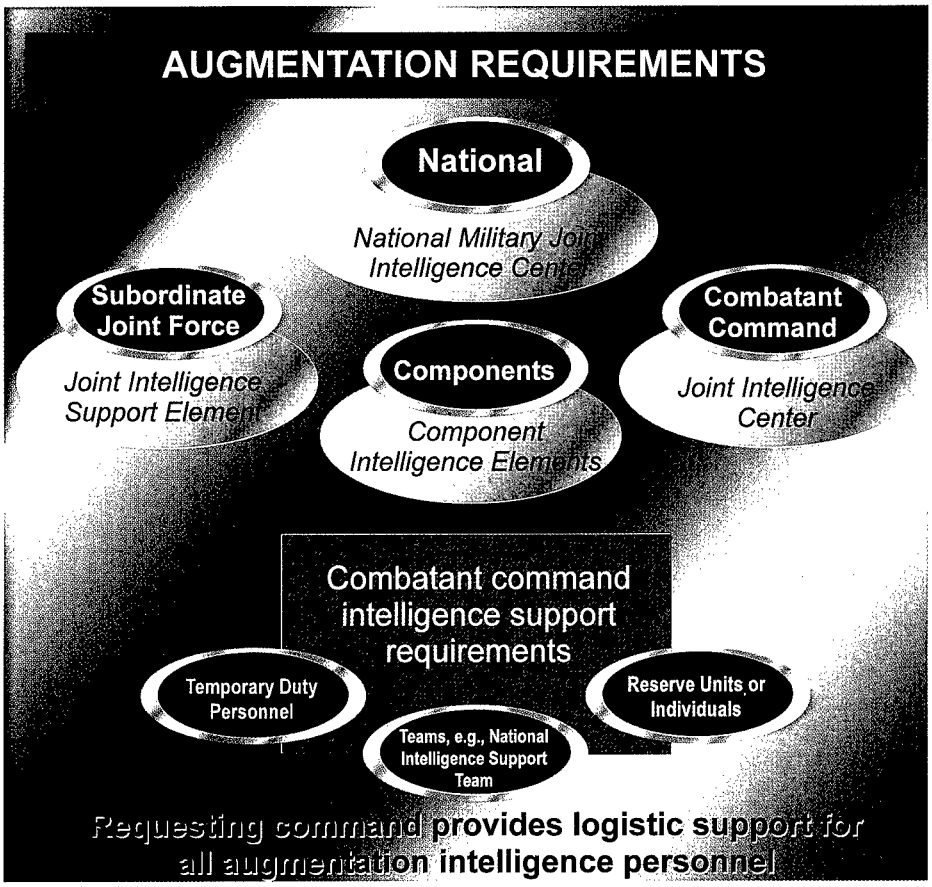


Figure III-4. Augmentation Requirements

national intelligence agencies and tailor the composition of the deployment packages to meet those needs. The combatant command J-2 may integrate these supporting capabilities with the command's JIC and the subordinate joint force JISE. The deployment packages, including NIST and HOC, provide access to the entire range of capabilities resident in the national intelligence agencies and can focus those capabilities on the JFC's intelligence requirements.

7. Intelligence Requirements

Successful intelligence support to military operations demands that some **universal principles** be understood and applied.

a. **The J-2 participates fully in the planning and decision making process**, contributing knowledge concerning the battlespace and the threat and receiving guidance to help focus the intelligence effort. The intelligence planner examines tasks and subtasks, then determines what intelligence support and information will be required to achieve mission success.

b. In the course of mission analysis, **the intelligence planner keeps in mind the kinds of intelligence required**. Mission analysis leads to the development of the commander's PIR, as recommended by the J-2. The categories, types, and level of detail required for intelligence analysis differ from

echelon to echelon. Intelligence necessary to support a theater-level mission might be inappropriate for a smaller-sized element in the field or at sea, while intelligence valuable at the national level might be irrelevant for a combatant command. **With some exceptions, the higher echelon commander's intelligence requirements are a less detailed subset of the subordinate commanders' requirements, although they are of a much broader scope.** An intelligence planner who tries to use intelligence beyond what is required to support the organization may overburden the intelligence infrastructure with too much information and needlessly complicate the commander's decision making process.

c. **Requests for information (RFI) respond to customer requirements,** ranging from dissemination of existing products through the integration or tailoring of onhand information to scheduling original production. The information must be timely, accurate, and in a usable format. The intelligence office translating the customer's requirement and the primary intelligence producer determine how best to meet the customer's needs. If it is determined that new, finished intelligence derived from original research is required to satisfy all or a portion of the RFI, then that need is expressed formally under Department of Defense Intelligence Production Program (DODIPP) as a production requirement (PR).

- Requirements that cannot be satisfied are submitted as RFIs or collection requirements to the next echelon. Each echelon is responsible for validating, prioritizing and, if possible, satisfying the RFI or collection requirement before forwarding it to the next level. (Figure III-5) **RFIs should be satisfied at the lowest level. If the information required to satisfy an RFI does not exist**, the requester is informed and a decision is made to initiate collection and/or production. Decisions to expend collection resources should be made at the lowest level possible.

- **Validation**, a process associated with the collection and production of intelligence, **confirms that a requirement is appropriate and has not been previously satisfied**. Information copies of the requirement should be forwarded to supporting intelligence organizations to

Special Operation Forces Intelligence Requirements

SOF intelligence requirements are heavily mission- and situation-dependent. SOF supports the Services in special reconnaissance, combating terrorism, counterdrug, and combat search and rescue and/or personnel recovery missions. SOF missions applying direct military force concentrate on attacking or collecting information on critical targets. SOF indirect missions include unconventional warfare, foreign internal defense, psychological operations, civil affairs, security assistance, and humanitarian assistance and/or disaster relief and peacekeeping operations.

SOF intelligence needs focus on leveraging the social, economical, political, and psychological conditions within a targeted country or area to US benefit. Development and maintenance of a good rapport with host-nation governments and indigenous population groups are essential to successful mission accomplishment. To establish that rapport, SOF soldiers require extensive knowledge of the local populace and its culture, language, religion, and customs. Unconventional warfare requires information on the presence and viability of subversive movements, including the populace's likely response to government actions.

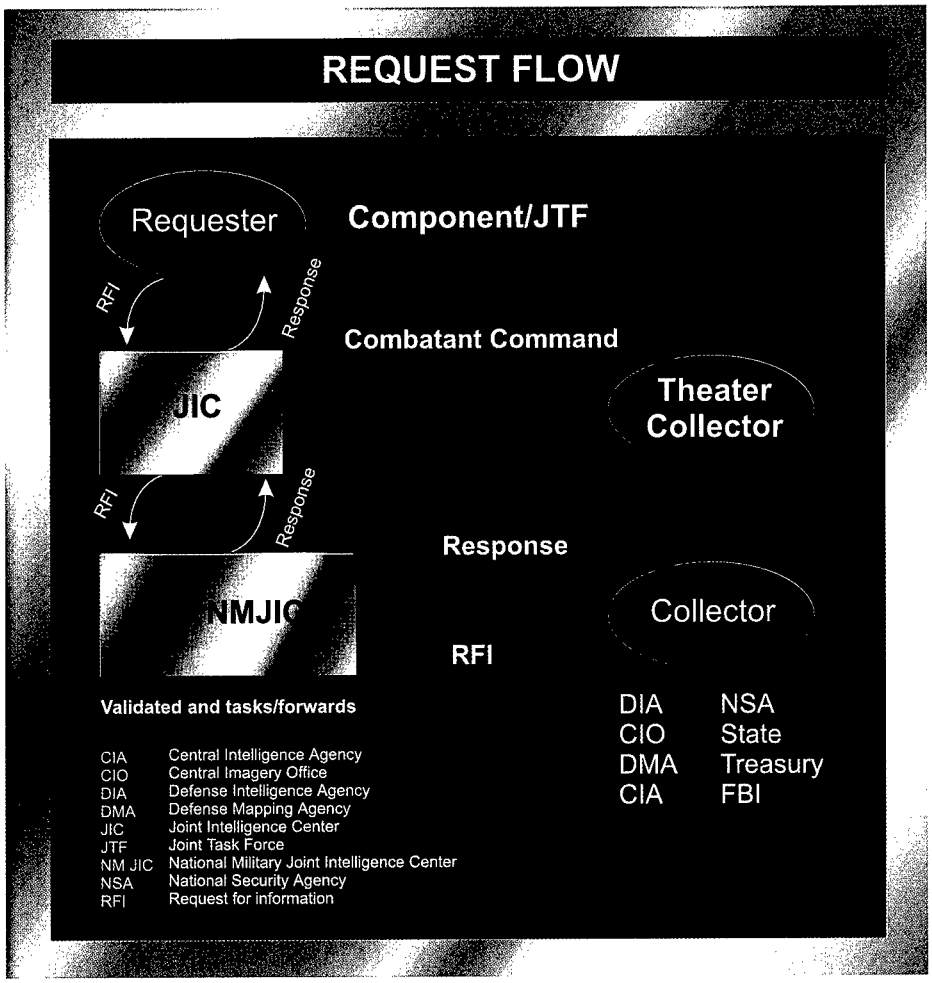


Figure III-5. Request Flow

alert potential respondents to the requirement. This provides them additional time to prepare a response and allows those with partial answers to contribute.

8. Evaluation

The success of the planning and direction phase can only be determined by the results achieved in the other phases of the intelligence cycle. The efforts of the unified command and/or subordinate joint force J-2s during planning and direction can positively affect the rest of the cycle.

SECTION B. COLLECTION

9. Overview

a. **Collection operations acquire information about the adversary and provide that information to intelligence processing and exploitation elements.** Collection management, which occurs at all levels of intelligence, converts intelligence requirements into collection requirements; establishes, tasks or coordinates actions with appropriate collection sources or agencies; and monitors results and retasks as required. The

foremost challenge of collection management is to **maximize the effectiveness of limited collection resources within the time constraints imposed by crisis or wartime operations.**

b. The terms "collection asset" and "collection resource" need to be clarified in order to understand the collection management process and the appropriate tasking procedures. **A collection asset or a collection resource is a collection system, platform, or capability.** A collection asset is subordinate to the requesting unit or echelon, while a collection resource is not. **Requests for collection resources must be coordinated with the echelon that directs and controls them through the chain of command.**

10. Duties and Responsibilities of the Collection Manager

a. **Collection managers develop collection plans based on the intelligence requirements of commanders and decision makers.** Intelligence analysts support the collection management process by identifying intelligence gaps and collection opportunities. **The collection manager's task is to obtain the necessary information in response to the requirement.** To do this the collection manager ensures the following: (1) Develops and manages a collection plan that integrates requirements with target characteristics. (2) Compares the plan to the capabilities and limitations of the available organic collection assets. (3) Develops a collection strategy to optimize collection availability and capability

Figure III-6. Collection Managers and the Collection Plan

to collect against the target. (4) In coordination with the J-3, forwards collection requirements to the component commander exercising tactical control over the theater reconnaissance and surveillance assets. The component will then task the asset to satisfy the JFC requirement. (5) Identifies collection requirements that cannot be met by organic assets and forwards them up the chain of command for validation and tasking of intelligence resources. (6) Directs processing and dissemination of collected data. (Figure III-6) Collection managers must understand the capabilities and limitations of each discipline and the procedures for ensuring target coverage by the appropriate collection asset and/or resource. Collection managers should keep requesters informed of collection status and capabilities so that there are realistic expectations of what can be collected and what level of confidence can be placed in the information.

b. **The mission may require additional intelligence resources not organic to the theater or the components that are part of the subordinate joint force.** Acquiring the use of unique or limited intelligence collection systems, such as UAVs and the Joint Surveillance Target Attack Radar System with ground station module, requires coordination with theater, Service and national agencies. Requests should be fully coordinated with components, subordinate commands, JTF J-3 and J-2, the combatant command J-3 and J-2, the Services, and the Joint Staff J-3 and J-2. The Joint Staff J-3 and J-5 recommends approval of the request to the Chairman of the Joint Chiefs of Staff, who signs the formal approval message or document upon Secretary of Defense approval.

11. Principles of Collection Management

Collection managers should follow four principles in all collection considerations. (Figure III-7)

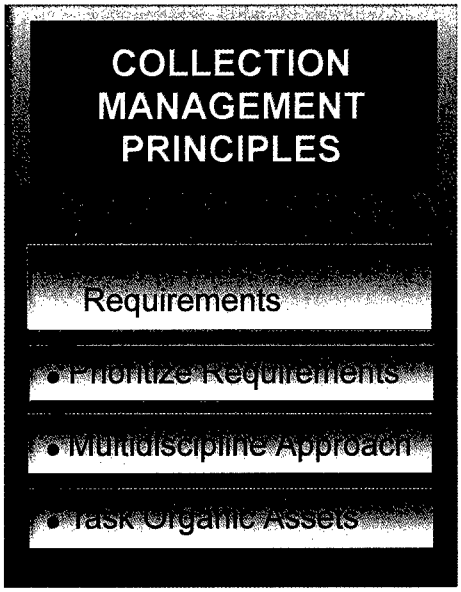
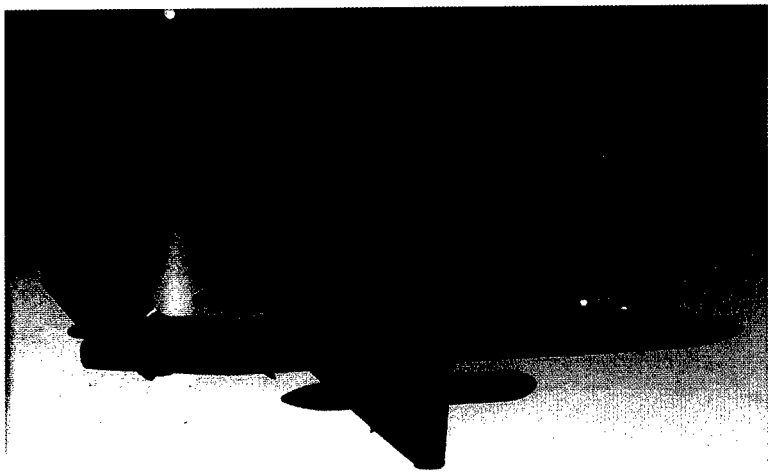


Figure III-7. Collection Management Principles

a. **Early Involvement. Collection managers should be involved early in the identification of requirements.** Early consideration of collection factors enhances the ability to respond in a timely manner, ensures thorough planning, and increases flexibility in the choice of disciplines and systems.

b. **Prioritization.** Prioritization **assigns distinct ranking to each collection requirement**. Collection decisions can be made rationally only if requirements are prioritized and the resulting trade-offs are fully understood. Time constraints and the finite number of collection, processing, and production assets and/or resources mandate prioritization of collection requirements. Prioritization, based on the commander's guidance and the current situation, ensures that limited assets and/or resources are directed against the most critical requirements.

c. **Multidiscipline Approach.** Collection disciplines complement each other, and the collection manager must resist favoring or becoming too reliant on a particular



Flexibility in collection coordination is key to good management; the tools of intelligence collection should be utilized to the best of their ability.

discipline or system. **Each discipline's limitations can be mitigated through the capabilities of the others**, as different systems provide additional insights into the requirement. While a sensor, discipline, and/or system may seem to be an obvious choice to satisfy a requirement, flexibility is the key. Rigid dependence on a single source may result in mission failure, especially if that source becomes unavailable. Lack of a multidiscipline approach may also result in discernible patterns that may play into the adversary's CI or camouflage, concealment, and deception (CCD) efforts. The HUMINT, IMINT, SIGINT, measurements and signature intelligence (MASINT), and open source intelligence (OSINT) disciplines are described in Appendix C, "Intelligence Disciplines."

d. **Task Organic Assets First. Use of organic collection assets allows a timely and tailored response** to collection requirements and serves to lessen the burden on collection resources controlled by other units, agencies, and organizations. However, if requirements cannot be satisfied by organic assets, the collection manager should not hesitate to request collection support from higher, adjacent, and subordinate units, agencies, and organizations.

12. Collection Management

Depending on the size of the collection management element, the CRM and COM functions may not be organizationally distinct. Although considered separately to facilitate understanding of their different objectives, in practice the distinction between them may disappear. There must be a constant dialogue between the two. **The collection management model is used to depict and better understand the process of collection management. (Figure III-8)**

a. **Collection management has two distinct functions: CRM — defining what intelligence systems must collect; and COM — specifying how to collect.** CRM focuses on the requirements of the customer, is all-source oriented, and generally interacts with production elements. COM focuses on the selection of the specific intelligence discipline(s) and specific systems within a discipline to be used to collect information addressing the requirement. COM is less concerned with the content of what is collected

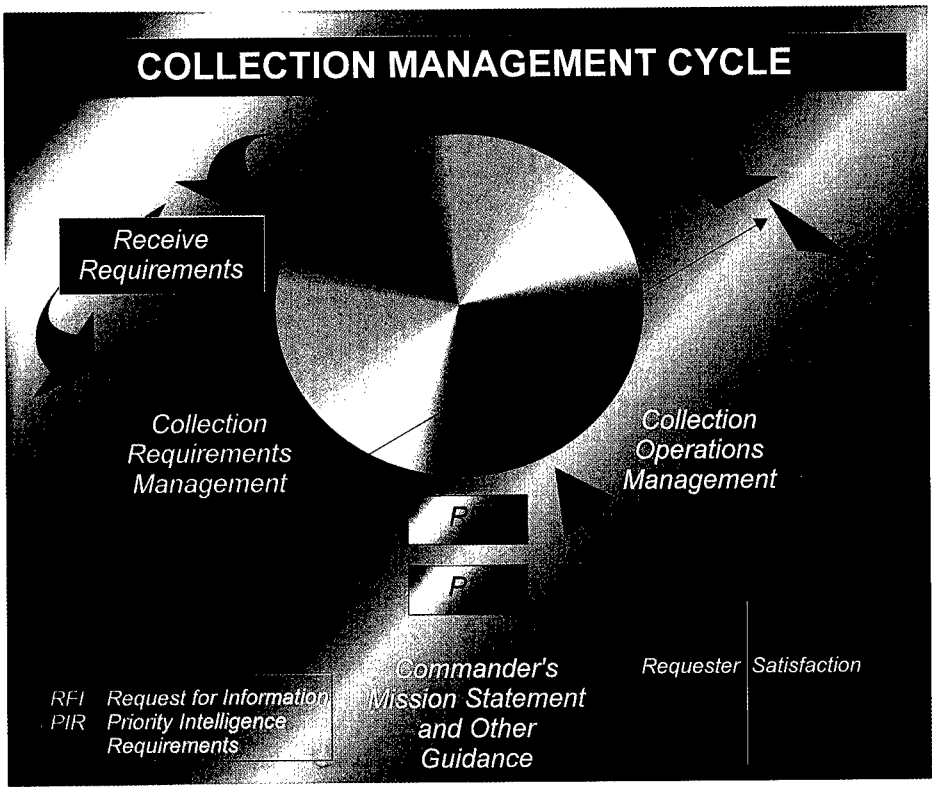


Figure III-8. Collection Management Cycle

than with determining how to collect against the requirement (collection strategy). COM is conducted by organizations within the various intelligence collection disciplines and is accessible to the operators of the collection system. (Figure III-9)

b. **COM and CRM are performed at all levels of the intelligence community.** Each level interacts with the levels above and below, and among units, agencies, and organizations on the same level. The further up the chain, the broader the perspective and scope of responsibility; the lower, the more specific the function and narrow the scope. Organizations possessing collection assets and/or resources perform COM.

Relationship Between Collection Management and Operations

The JFC controls all theater reconnaissance through the collection management function, if requirements exceed available assets. The JFC's collection manager prioritizes collection requirements and determines the appropriate asset to be assigned to collect against a particular target. The collection manager, in coordination with the J-3, forwards collection requirements to the component commander exercising tactical control over the theater reconnaissance and surveillance assets. A mission tasking order goes to the unit selected to be responsible for the accomplishment of the collection operations. The selected unit makes the final choice

of specific platforms, equipment, and personnel based on such operational consideration as maintenance schedules, training, and experience.

13. Military Collection Requirements

Responsibility for military collection requirements management at the national level rests with the DIA Directorate of Operations (DO). The DO ensures that all-source collection requirements and capabilities are tasked to provide operational policy and intelligence support to the NCA, Joint Chiefs of Staff (JCS), Office of the Secretary of Defense (OSD), the Services, combatant commands, and their components.

a. **To carry out these responsibilities, the DO coordinates and validates military collection requirements**, including managing time-sensitive, ad hoc high interest and crisis-related all-source collection requirements for the Department of Defense. The DO develops all-source collection postures, strategies, policy and procedures, including providing advice on these subjects to the Director, DIA and Chairman of the Joint Chiefs of Staff as required for crisis response, intelligence issues, and other special events; evaluates the results of collection activities; and develops and maintains collection requirements data bases and associated management systems.

b. **The DO provides liaison and representation to facilitate cooperation with other intelligence agencies.** The DO is the intelligence collection management interface with the Joint Staff Reconnaissance Center for the review, coordination, and conduct of sensitive reconnaissance

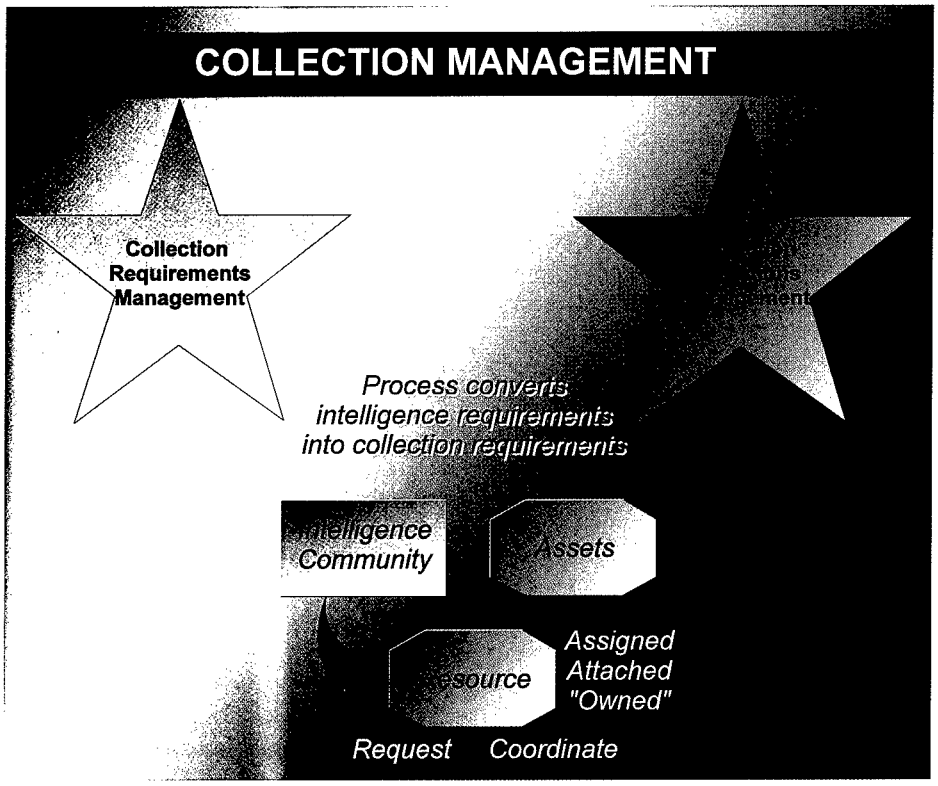


Figure III-9. Collection Management

operations program missions worldwide. Another function of the DO is to provide DOD and DIA representation on national-level forums charged with collection management and oversight responsibilities, such as the SIGINT Committee, as well as their subcommittees and working groups.

c. **In the event of war or periods of crisis, the President may direct the military to exercise greater responsibilities for tasking of collection systems.** When directed, national intelligence collection tasking authority may pass from the DCI to the Secretary of Defense. When this occurs, the DO manages this collection tasking authority. This collection tasking authority approves collection requirements, determines collection priorities, and resolves conflicts between collection priorities.

d. **Joint Staff J-2.** The other principal military member in collection at the national level is the Joint Staff J-2. **The J-2 coordinates the tasking of national technical reconnaissance systems and nationally-subordinated manned reconnaissance platforms and sensors.** As consolidated authority for central HUMINT tasking, the J-2 coordinates and levies DOD HUMINT tasking and coordinates with other agencies responsible for SIGINT, IMINT, MASINT, and other special collection programs as required. The J-2 also responds to RFIs submitted by subordinate elements and commands.

e. **Operations Management.** Each of the intelligence collection disciplines has a separate infrastructure to manage operations.

f. **Theater Collection Management.** The theater J-2 must be kept apprised of all intelligence collection requirements being levied on assets and resources within the combatant command's AOR. **The theater J-2 retains full management authority (i.e., to validate, to modify, or to nonconcur) over all intelligence collection requirements against targets and objectives within the AOR.** This authority may be delegated to a subordinate JFC. Collection requirements must be satisfied at the lowest possible level. Requirements that cannot be satisfied, and that have been validated by the command's collection manager or J-2, must be forwarded to the next higher echelon for action. This process continues until the requirement is satisfied, the intelligence is no longer needed, or it is determined that the requirement cannot be satisfied. Validated collection requirements and collection requests for theater and national systems will be forwarded for action to the theater intelligence collection management office. Validated collection requirements from components will become part of the theater collection plan and will be collected by theater collectors or forwarded to the DO.

14. Collection Requirements Management

Management and validation of collection requirement requests for a theater resides at the combatant command level. The validation process parallels that for RFIs and is responsive to operational requirements. The JIC validates and submits collection requirements to DIA if requirements cannot be satisfied by organic or subordinate resources.

a. **Requirements. The combatant command J-2 validates or modifies standing collection requirements submitted by subordinate joint force or component commands.** The subordinate joint force J-2 validates collection requirements and submits requests for additional collection assets to the combatant command J-2. The JIC tracks the status of research, validation, submission and satisfaction of all collection requests received, including subordinate joint force and other theater command requirements.

b. **Collection Planning**

- The compilation of collection requirements is the basis of the collection plan. **Collection planning is a continuous process that coordinates and integrates the efforts of all collection units and agencies.** The CRM cycle begins with initial efforts to answer the commander's PIR established during the planning and direction phase of the intelligence cycle. Based on the PIR, intelligence analysts prepare RFIs. In the context of collection management, RFIs are queries to see if the information already exists and, if not, they form the basis of a collection requirement and/or analysis. The collection manager checks any ongoing collection operation that might contribute to satisfying the requirement. This requires that collection managers remain cognizant of previous and ongoing collection efforts. When previously collected information will not suffice, collection requirements will be developed. When the RFI manager positively determines that the information is neither available nor extractable from archived information or from lateral or higher echelons, an intelligence gap is identified. It becomes the responsibility of collection management to obtain the information.

- The collection plan may be either a simple hardcopy or automated worksheet used solely by the intelligence staff or a more formal document, depending on the complexity of the requirements to be satisfied. **The collection plan includes statements of information desired, when the information is needed, who is to receive the finished intelligence, and how it is to be used.** The answers collected to satisfy these requirements answer the PIR. The completed collection plan forms the basis for further collection actions. (Figure III-10)

- After establishing a collection plan, a strategy is created to obtain the information. The CRM transforms each requirement from the plan into a specific effort that ensures optimum employment of limited collection capabilities. For efficient management of collection requests, it is important to create a registry of active, prioritized

COLLECTION PLAN FORMAT					
Period Covered: From_____ To_____					
PIR or Other Intelligence Requirements	Indications	Specific Information Sought	Assets to be Tasked/ Resources to be Required	Place and Time to Report	Remarks

Figure III-10. Collection Plan Format

requirements and to continuously update and monitor it from inception to satisfaction or termination.

c. **Resource Availability and Capability.** After defining the requirement, **the collection manager determines the availability and capability of collection assets and resources that might contribute to requirement satisfaction**. The information sought is examined for discrete elements, called specific information requirements (SIRs). A requirement may have more than one SIR. For each SIR, a set of key elements is developed that can be used to compare characteristics of the requirement's target with the characteristics of available assets or resources to determine collection suitability. Capability factors are shown at Figure III-11.

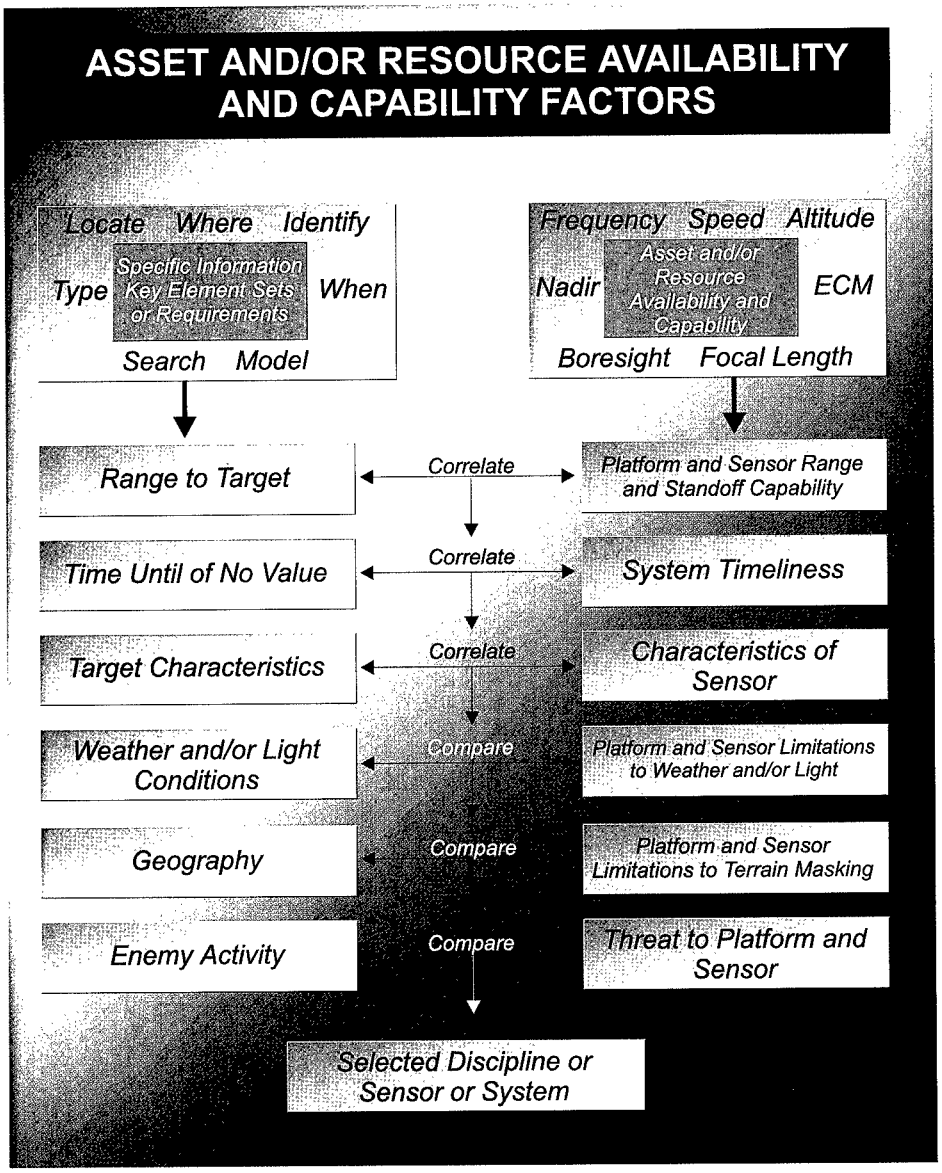


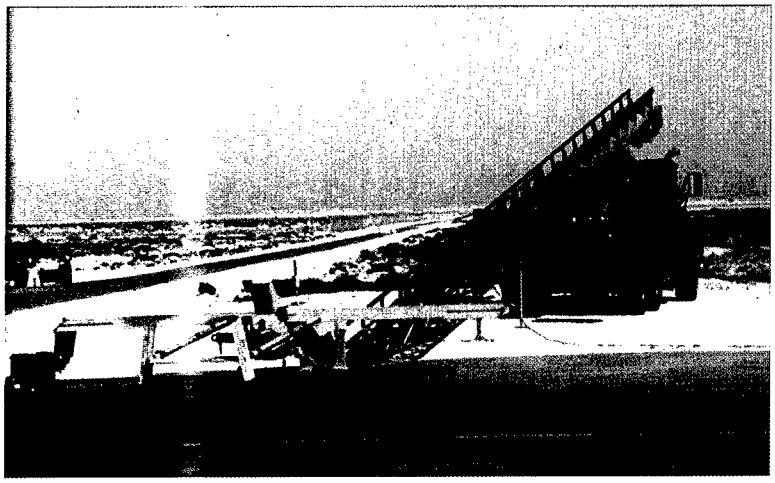
Figure III-11. Asset and/or Resource Availability and Capability Factors

- **Key Element Sets.** Key elements are the parameters of the target's characteristics that can be compared with the characteristics of the available assets and/or resources and serve as discriminators in discipline and/or sensor selection. A complete set of key elements provides the basis for identifying sensors fully capable of performing the collection task. **The key elements commonly considered are: target characteristics, range to the target, and timeliness.**

  •• **Target characteristics are the discernible physical, operational, and technical features of an object or event.** These characteristics may be observable and/or collectible. Observables are the unique descriptive features associated with the visible description of the target, whether it is specific units, equipment, or facilities. Collectibles are the unique descriptive features associated with emanations from the target. Observables are associated with IMINT and HUMINT/CI, collectibles with SIGINT, and both are associated with MASINT. One or more target characteristics may be associated with a specific information requirement, and these characteristics can be compared to a sensor(s) capability to collect. By continuing this process for each of the collection disciplines, a complete key element set is developed for the target.

  •• **Range is measured as distance from a predetermined reference to the target location.** The range to the target can be used to quickly eliminate from consideration both those standoff sensors that are unable to cover the target area and those sensors on penetration platforms not capable of reaching the target area. In HUMINT/CI, the analogous consideration would be source access.

  •• **Timeliness is when the information requested must be received in order to be of value.**



A collection manager may determine that the risks involved in intelligence collection dictate the use of an unmanned aerial vehicle.

- **Collection Capabilities Factors.** The CRM translates the capabilities and limitations of the available sensors, systems, or disciplines into a set of collection capability factors that can be

directly compared to the key element sets. The capabilities and limitations of various disciplines and systems are considered, together with their availability, to decide whether or not they should be tasked. **Sensor capability factors are technical or performance characteristics, range, dwell time, and timeliness.**

•• **Performance characteristics** are concerned with the system's ability to collect the requested information, output quality, and location accuracy. (1) A system within a particular discipline may or may not be able to collect information on a particular target. For example, SIGINT collection systems operate in discrete frequency ranges, so that if the adversary system being sought operates outside those ranges, that particular collector is not viable as a potential source. (2) The data quality relates to the level of detail that can be derived from the collected information. For example, different imagery systems provide varying degrees of image resolution. (3) The importance of location accuracy depends on the planned use of the information collected. For example, information collected for targeting purposes demands greater locational accuracy than information collected for updating OB.

•• **Range** deals with the system's ability to provide target coverage. For airborne systems, range is determined by considering the actual range capabilities of the sensor to provide detailed information sufficient to satisfy the requirement and the restrictions placed on the airborne platform. The CRM assesses combinations of these various range factors in order to determine a sensor's potential to meet operational requirements.

•• **Dwell time** is the length of time a given collector can maintain access to the target, an important consideration in monitoring and/or changing detection scenarios.

•• **Timelines** consider the time required to complete each collection event, and is calculated or estimated for each available sensor based on the tactical situation and the local circumstances. (Figure III-12) Times vary depending on mission priority assigned, specific system availability, time required to plan the mission, and related information

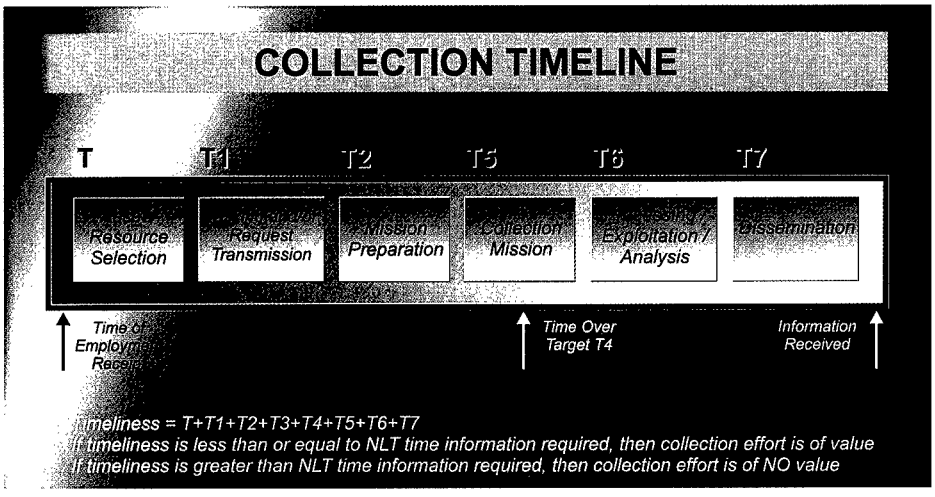


Figure III-12. Collection Timeline

processing and dissemination means. These times are added to find an overall elapsed time, then compared with the latest timeliness information stated by the user. If the system's timeliness exceeds the latest time of receipt when the information collected will be usable, then it fails to contribute to satisfying the specific requirement and should not be considered for collection planning purposes.

- **Correlation.** Correlation is **the process which associates and combines independent data on a single subject to improve the reliability or credibility**. Key element sets are compared with collection capability factors to provide a preliminary list of sensors that are technically able to collect the desired data within the range to the target and time required.

- **Environmental Factors.** After correlation, the candidate sensors are compared with environmental factors to support final sensor selection. **Environmental factors are the threat, terrain, and weather** that might influence the particular discipline or sensor selection. Depending on the environmental factors, a technically capable sensor may be dropped from consideration.

  •• **Sensor vulnerability is the degree to which adversary countermeasures will affect sensor selection and depends on the vulnerability of the sensor platform.** In general, the platforms of penetrating sensors are the most vulnerable, stand-off sensors less so, and satellite sensors the least vulnerable. Threat assessment is an evaluation of risk (military risk and political sensitivity) versus intelligence gain.

  •• **Weather and light conditions are a consideration**, particularly with IMINT sensors. Weather conditions in and around the collection area affect the sensor capability to collect and exploit data.

  •• **Terrain is also a consideration.** It may mask a target, thereby dictating the direction a sensor must point.

- **Availability.** The list of viable collection disciplines, systems, and sensors is reviewed for current availability and the addition or deletion of capabilities. Coordination with adjacent and higher headquarters will determine the availability of theater and national resources.

d. **Task Assets or Request Tasking of Resources**

- The collection manager begins by considering the highest priority requirement, then proceeds through the active requirements list to determine how each request can be satisfied. (Figure III-13) **CRM transmits to COM requirements and recommendations for planning, scheduling, and control of the prioritized list.** The resulting tasking provides specific guidance that identifies the activity to undertake collection operations, the target to be covered, the date-time the mission is to be accomplished, and the place and time data is to be reported. Collection tasking includes processing and exploitation tasking, guidance, and instructions.

- **Collection to satisfy the requirement may occur at any level.** For example, if a combatant commander determines that the information needed to answer a RFI is unavailable, the commander may task organic collection assets or those of a subordinate organization or request coalition or national-level support to satisfy the requirement. When preparing the tasking and/or request, consideration

COLLECTION TASKING WORKSHEET

Organization: Registration Number:

DTG: Collection Manager:

Specific Information Requirements: _____

Time:_____ Target Range:_____

Characteristics: _____

Assets/ Resources	Range	Timeliness	Characteristics	Weather	Geography	Threat	Capability	Remarks
HUMINT								
CI								
IMINT								
COMINT								
ELINT								
MASINT								
OSINT								

Assets/Resource Selected HUMINT: _____ COMINT:_____ MASINT:_____ CI:_____

IMINT:_____ ELINT:_____ OSINT:_____

Figure III-13. Collection Tasking Worksheet

should be given whether to integrate the requirement into an ongoing, planned, or new mission. This subject is discussed further below, under intelligence collection strategy.

- **Tasking request forms or messages are dependent on the tactical situation, type of sensor, and type of asset or resource** (i.e., organic, supporting, theater, national, or multinational). Many specific data elements in these requests and the transmission procedures are classified. In the case of organic and direct support assets, requesters follow combatant command instructions provided in the OPLAN or OPORD intelligence annex, or by message. In addition, the Joint-Service Tactical Exploitation of National Systems Manual and the DIA 58-series manuals provide guidance for requesting support from national resources. In preparing requests for national resources, the collection manager should consider the guidelines in Figure III-14.

GUIDELINES FOR REQUESTING NATIONAL RESOURCE COLLECTION	
Areas of Interest	National systems are best employed agains high-priority targets outside the range of organic or theater sensors, beyond standoff collection range, and/or in high threat areas.
Exploitation and/or Analysis Timeliness	Targets must be chosen such that, under applicable timeliness constraints, exploitation reports will reach the commander in time to react or influence decision making.
Justifications	Request justifications must fully explain the need for information and support the priority assigned by the requester.
Sensor Capabilities	Target descriptions must place minimum restrictions on systems' use.
Sensor Accessibility	The targets' accessibility must be determined when possible before a collection request is forwarded.
Exploitation and/or Analysis Requirements Clarity	Exploitation and/or analysis requirements must be concise, explicit statements of the actual information needed.
Exploitation and/or Analysis Requirement Purpose	Exploitation and/or analysis requirements must state the purpose of the information desired when it will benefit the interpreter and/or analyst.
Preplanned Collection	Preplanned target sets submitted in advance of an operation can relieve the workload and must be considered where the tactical situation permits.

Figure III-14. Guidelines for Requesting National Resource Collection

- **Intelligence Collection Strategy**

  •• A collection strategy is a systematic scheme to optimize tasking of all capable and available collection assets and/or resources against requirements. The collection strategy considers all outstanding intelligence requirements, their relative priority, and the immediate tactical situation.

  •• **Resource integration is a process whereby a new collection requirement is integrated with current or planned missions to increase the efficiency of the overall collection effort.** By tasking a mission already in progress, it may be possible to reduce timelines, make collection more responsive to the request, and decrease cost and risk. This is weighed against the priority of scheduled targets that may have to be dropped to accommodate new targets and the impact of a mission change on the effectiveness of the ongoing mission. When other means of collection are unavailable or impractical, a new mission should be planned based upon the new request.

  •• While one source may be suitable to collect against different requirements, in some cases multiple sources are necessary to satisfy a single, high priority requirement. **Cueing is the use of one discipline or sensor to target collection by another sensor.** Cueing could be within the same discipline, where a wide-area sensor tips off to a point-target sensor, or it could be cross-discipline, where one discipline tips off another discipline.

  •• **Asset mix and/or redundancy uses a combination of assets of differing disciplines (asset mix) or similar disciplines (asset redundancy) against a high priority target.** When the probability of success of one sensor to completely satisfy the requirement is lower than acceptable, the use of multiple capabilities of different systems or disciplines increases the likelihood of success. Asset mix or redundancy places greater demands on the limited assets and/or resources available and has to be clearly justified by the potential intelligence gain.

e. **Evaluate Reporting.** The evaluation process **tracks the status of collection requirements and provides feedback to the requesters**. Monitoring outstanding requirements ensures that orders and requests to collection activities are understood and the right information is being sought. When the collection results are provided, the collection manager evaluates the report(s) for completeness, ensures that the requesters receive a copy, and determines if the requirement has been satisfied. Requester feedback establishes customer satisfaction, permits tasker deletion and frees collection assets and resources to be redirected to satisfy other active requirements.

f. **Collection Plan Update.** Based on the requester's assessment of requirement satisfaction, **the collection manager reviews priorities for currency**. The collection plan is updated to include retasking (if the requirement is not satisfied), adding new requirements, or canceling satisfied requirements.

15. Collection Operations Management

The COM process organizes, directs, and monitors the equipment and personnel that actually collect the data to satisfy requirements. COM develops strategies for collection against requirements in cooperation with CRM; predicts how well a system can satisfy requirements; evaluates the performance of the collection systems; allocates and tasks collection assets and/or

resources and processing and/or exploitation systems; and monitors and reports the operational status of collection systems. (Figure III-15)

a. **Collection Mission Planning**

- **Planning is concerned with the identification, scheduling, and controlling of collection assets and/or resources.** The operations planner reviews mission requirements for sensor and target range, system responsiveness, timeliness, threat, weather, and reporting requirements. These elements are considered with the detailed technical, administrative, and logistical data of the collection system to identify and determine asset and/or resource availability and capability. The requirements are then translated into specific mission tasking orders.
- **Effective coordination is vital in mission planning operations.** With aircraft collection platforms in particular, many different staff elements are involved: operations, weather, maintenance and logistics, and communications must all be closely integrated into the mission planning effort. Intelligence sensor planners and managers of processing and exploitation elements must fully understand the requirements and mission profile. It is strongly recommended that COM personnel and resources be located in proximity to the operations staff elements which are responsible for reconnaissance assets.

b. **Execution.** A mission tasking order goes to the unit selected to be responsible for the accomplishment of the collection operation. The selected unit makes the final choice of specific platforms, equipment, and

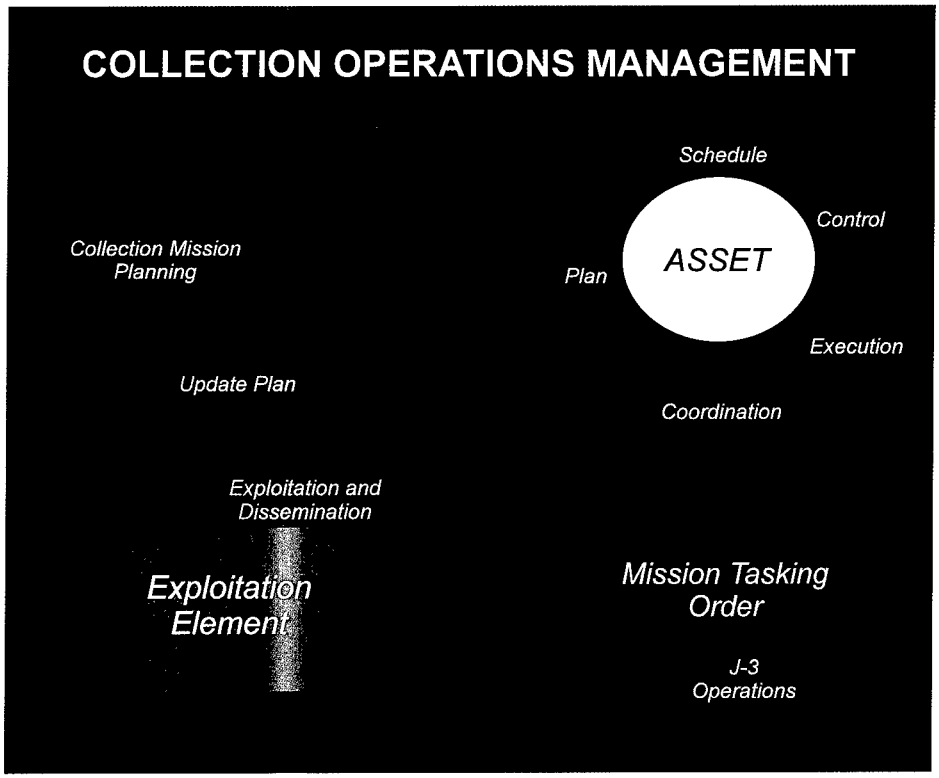


Figure III-15. Collection Operations Management

personnel based on such operational considerations as maintenance schedules, training, and experience.

c. **Exploitation.** Exploitation of collected information is closely associated with the management of collection assets and resources. Generally the staff allocated a collection capability also controls the sensor-unique processing, exploitation, and analysis equipment. Exploitation is discussed further in Section C and dissemination in Section E of this chapter.

d. **Collection Planning Update. Following exploitation, the report or processed data is disseminated to the requester.** If the data is insufficient, the requester coordinates with the collection manager for additional coverage. At this point, the processed requirement transitions back to the CRM function. The collection manager and the exploitation manager, in coordination with requesters, continually assess how collection operations quality and timeliness may be improved. This effort relies heavily on those supporting organizations and other units or agencies that own and operate collection and exploitation assets or resources.

THE CAPTURE OF THE GERMAN ROCKET SECRETS

Early in 1929, German engineers had begun studying rocket and jet propulsion to be used for transporting mail. In 1933, when Adolf Hitler became Chancellor, these studies were shifted to military uses, and the scientists were instructed to explore all ideas, however fanciful. Huge sums were made available to the Speer Ministry, where Dr. Wernher von Braun and a group of scientists conducted rocket research. The research enabled the "doomsday" weapons of the era to be produced, the best known of which were the V-1 and V-2 missiles.

In the Spring of 1945, as the outcome of WW II in Europe became more and more apparent, a principal focus of US intelligence units in Europe was to capture all possible information pertaining to rocket weapons. Accordingly these units followed closely behind advancing Allied forces, particularly in the Black Forest area where technical personnel with key documents from the Speer Ministry had scattered under heavy pressure of aerial bombing in Berlin. It was up to the intelligence units to find these individuals and gain information from them. The search began by interrogating the Germans who were in custody as a result of the Allied advance.

This method of collection, while painstaking, proved fruitful. Through such interrogations US intelligence officers learned that the former director general of German rocket production, George Richkey, was in captivity, working in a salt mine in the Black Forest. The following is the account of Norman Beasley, who told the story of his brother, Colonel Peter Beasley, the senior intelligence collection officer in the area.

"'I've got a job for you that is different than working in the salt mine,' Colonel Beasley told Richkey at the first interrogation. 'I want you to begin right now writing out a full description of yourself and all the activities of the V-2 factory.'

When Richkey's report was completed, Colonel Beasley made it clear, 'we accept you as an official of the German Government; we have patience and

time and lots of people—you have lost the war and so as far as I am concerned you are a man who knows a lot about rockets. As an American officer, I want my country to have full possession of all your knowledge. To my superiors, I shall recommend that you be taken to the United States.'

Richkey nodded his assent, explained he was a scientist and wanted only to develop his knowledge in pleasant surroundings, such as the United States, and agreed to tell where the records were hidden, and to show the colonel the place.

Only hours later, under a heavily armed escort, Richkey led Colonel Beasley into the Black Forest to a cave, 5 feet wide and 5 feet high, running 300 feet into a mountain. There, records were found intact. Upon examination, the records disclosed basic blueprints, worksheets, engineering tables, and advanced plans for virtually every secret weapon in the possession of German scientists."

SOURCE: Norman Beasley, *The Capture of the German Rocket Secrets* Military Intelligence: Its Heroes and Legends, compiled by Diane L. Hamm US Army Intelligence and Security Command History Office, October 1987

SECTION C. PROCESSING AND EXPLOITATION

16. Overview

a. **During processing and exploitation, collected data is correlated and converted into forms suitable for analysis and production.** In this step the data **may be further exploited to gain fullest possible advantage from it**. Processing remains distinct from the production phase of the intelligence cycle in that the data is not yet fully subject to analytical assessment.

b. **At the combatant command level, the J-2 manages theater processing systems and capabilities.** The J-2 should be prepared for system interoperability problems that may be experienced in a multinational environment and in operations with non-military and nongovernmental organizations and be flexible in developing work-around procedures. Processing elements should be prepared to set up both US only and coalition segments. At the subordinate joint force level, the deployable intelligence processing elements oversee interoperability of systems and manage assignment of joint capabilities as required to support the JFC.

c. Processing and exploitation of collected information by tactical units is closely associated with the management of collection assets. Normally, the collection operation element also controls the sensor-unique processing, exploitation, and analysis equipment. Various exploitation capabilities exist to service several different collection systems. **The exploitation manager must plan the workload and develop a priority system for accomplishing the work. This will ensure priority processing and exploitation during periods of high-volume collection activity.** (Figure III-16)

17. Processing and Exploitation of Human Intelligence

Processing of HUMINT/CI information primarily involves report preparation by collection activities at both the joint force and component levels. At the joint force level, this processing may also be accomplished within the J-2X. Further processing of human resource reporting is

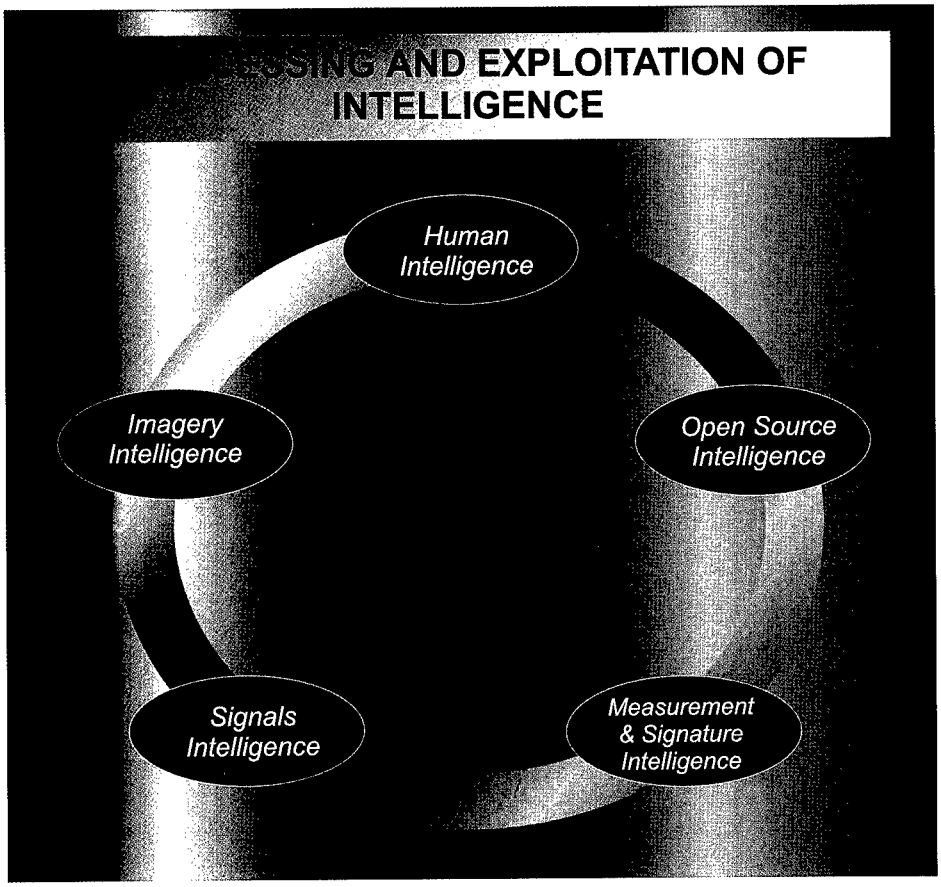


Figure III-16. Processing and Exploitation of Intelligence

conducted by the JIC and joint force analytical and/or production activities; this primarily involves analyzing HUMINT/CI reporting for inclusion in all-source production and/or for data base maintenance. Additionally, components of the joint force may consider document exploitation and translation as HUMINT processing activities IAW Service doctrine. Exploitation of HUMINT information provides knowledge of "intentions of key personnel/leadership" and CI can be used for indications and warning (I&W) and force protection.

18. Imagery Intelligence Processing and Exploitation

The JIC processes and exploits imagery in theater. The theater facility processes the digital signal and displays the downlinked imagery on a workstation in softcopy form for immediate exploitation. The imagery can also be stored on tape, sent to a digital archive for later use, or laid down on film for exploitation on a light table. The results of the exploitation and the annotated images may be incorporated into an all-source

HUMINT AND TARGETING

Identifying military targets was difficult [during DESERT STORM]; however, information acquired by HUMINT operations improved targeting and destruction of significant military facilities in Baghdad, including the MOD and various communications nodes. In addition to blue prints and plans, HUMINT sources provided detailed memory sketches and were able to pinpoint on maps and photographs key locations, which subsequently were targeted.

Sources detailed the locations of bunkers underneath key facilities, including the Iraqi Air Force headquarters, which was composed of several main buildings and five underground bunkers, and the Iraqi practice of stringing coaxial communication cable under bridges rather than under the river beds in Baghdad and southern Iraq. This information was the deciding factor in the decision to target key bridges in Baghdad. Sources identified the communications center in Baghdad; less than 12 hours later, this facility was destroyed. Information obtained from EPWs also helped planners direct effective air attacks against troops and logistics targets.

SOURCE: Final Report to Congress
Conduct of the Persian Gulf War, April 1992

product focusing on a given target or target type, topic, or activity. The IMINT data may also be used to update a data base. The result of the non-time-dominant exploitation may be a hardcopy report, tape media mailed or couriered to the user, or a softcopy.

19. Signals Intelligence Processing

SIGINT support to joint operations includes communications intelligence (COMINT), electronics intelligence (ELINT), and foreign instrumentation signals intelligence. **COMINT processing is accomplished by NSA/CSS elements either assigned to or in support of the joint force mission.** Depending on the level required for subsequent analysis and reporting, processing may be performed by assigned units in the operational area, at the regional JICs, or by specialized Service component or Defense activities. **ELINT processing in support of a joint force may come from a number of sources** including: assets attached to the joint force, national ELINT centers, the JC2WC, and combatant command JICs. A request through the theater J-2 to the NMJIC will result in tasking of appropriate organizations.

20. Measurement and Signature Intelligence Processing

MASINT tends to be a processing intensive collection discipline. It requires translating events (seismic, acoustic, radio frequency, infrared, and other events) into targeting intelligence (e.g., location, type of target). The Central MASINT Office and Service intelligence centers process MASINT. The Service scientific and technical intelligence (S&TI) centers provide a critical role in processing, analyzing, and exploiting MASINT data. They develop the initial processing techniques, validate the performance and accuracy of these techniques, and then create signature profiles of the desired targets. The targeting intelligence is then provided to the warfighter. **Currently, neither the theater JICs nor the subordinate joint force elements have the capability for MASINT processing.**

21. Open-Source Intelligence Processing

OSINT processing transforms (converts, translates, and formats) text, graphics, sound, and motion video in response to user requirements. For example, at the national level, the Foreign Broadcast Information System provides translations of foreign broadcast and print media.

22. Evaluation

Processing and exploitation, while difficult to evaluate separately from production, are "sensor" specific. Production, even sole source, is based on multiple sensors or sources.

SECTION D. PRODUCTION

23. Overview

a. Production is accomplished in response to expressed and anticipated user requirements and within assigned AORs and/or JOAs. Intelligence (in the form of both products and services) responds to: the chain of command and the decision making authority it supports; US policy decisions and military operational requirements; and changes in strategy, tactics, equipment, and overall capabilities of US and foreign military forces. Fused joint intelligence assessments, such as military capabilities assessments, military-related subjects assessments, or adversary COA assessments, are also frequently used to present the commander with the most thorough and accurate description and analysis of adversary status and intentions.

b. **Intelligence production is the integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence.** Intelligence production must be coordinated and directed by the J-2 to provide non-duplicative all-source intelligence products to the requester. **Production for joint operations is accomplished by organizations at every echelon from national to subordinate joint force level.** Effective production management ensures that the combatant commander and/or JFC receives the intelligence products and services required to accomplish the assigned mission. Automated data base systems provide current tailorable data appropriate to the mission.

24. Products

Intelligence products produced by or for the subordinate joint force are described below and in Figure III-17.

a. **Indications and Warning**

- The I&W process **analyzes and integrates operations and intelligence information to assess the probability of hostile actions and provides sufficient warning to preempt, counter, or otherwise moderate their outcome.** The focus of I&W varies at each echelon, and is most specific at the operational and tactical levels.

- Subordinate joint force I&W relies on tip-offs from all sources at all levels. An integrated and responsive intelligence architecture must be established to satisfy theater requirements. I&W intelligence requirements include the following:

  •• Local or regional government capability to deal with the situation.

  •• Adversary intentions, capabilities, preparations, deployments and related activities, and possible methods of attack.

  •• Adversary motivations, possible triggering events, goals and objectives.

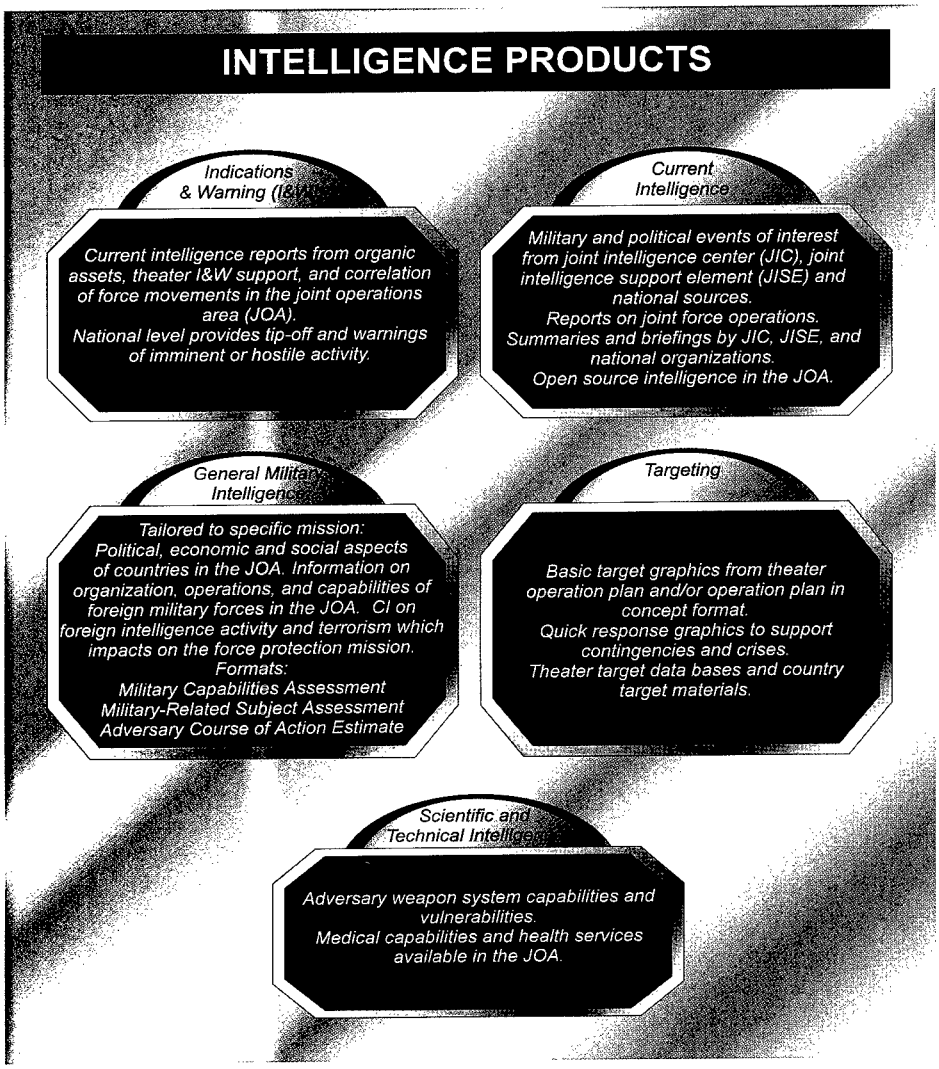


Figure III-17. Intelligence Products

•• Changes in adversary force dispositions, military activities, and mobilization status.

•• IW capabilities in the region.

•• Required military and civil mobilization preparations prior to military action taking place.

•• Non-military activity that could alter the situation, such as drastic changes in either friendly or opposing forces' political, economic or social situations.

•• Status of other military forces in the JOA.

b. **Current Intelligence**

- **Current intelligence involves producing and disseminating all-source intelligence on the current situation in a particular area.** It is similar to I&W in that both

depend upon continuous monitoring of world events and specific activities in the combatant command's AOR/JOA. The subordinate joint force receives current information from all levels of the intelligence community. This information consists of message traffic on military and political events of interest generated by the combatant command JICs, the subordinate joint force JISE, and national sources; real time reporting of operational situations by subordinate joint forces; summaries and briefings prepared by JICs, JISEs, and national-level organizations; and radio and television broadcasts in the JOA monitored by the subordinate joint force.

- During the warning and planning phases of an operation, the subordinate joint force J-2 should assess the adequacy of intelligence provided by the combatant command JIC and available through networked data bases and submit prioritized RFIs to satisfy immediate intelligence needs and gaps in coverage. Once the operation begins, the subordinate joint force's collection assets will be supplemented by theater and national support, to provide the joint force with current intelligence for use in intelligence assessments. Information required includes, but is not limited to the following:

  •• Adversary intentions and will to use military force, where, when, in what strength, and with what forces and weapons.

  •• The adversary's operational plans.

  •• The adversary's centers of gravity.

  •• The adversary's vulnerabilities.

  •• Analysis of the operational area including terrain, hydrology, infectious disease and environmental factors, manmade features, and demographics.

  •• Current and forecast METOC conditions which include the entire range of atmospheric phenomena extending from the earth's surface (cloud cover, precipitation, winds, and other METOC conditions) into space (space weather), as well as all of the marine environment from the bottom of the ocean to the air and/or sea interface (surf, sea conditions, or other sea interfaces).

  •• Military and political events.

  •• Status of strategic transportation nodes, to include major airfields, seaports, and surface networks.

- Current intelligence and general military intelligence (GMI) efforts are interdependent. The intelligence gained during development of current intelligence forms the basis for the GMI effort.

c. **General Military Intelligence**

- **GMI includes pertinent information concerning the political, economic, and social aspects of foreign countries as well as all information on the organization, operations, and capabilities of selected foreign military forces.** GMI is tailored to specific subordinate joint force missions. Specifically, GMI deals with information on the items listed in Figure III-18.

- Fused joint intelligence assessments are listed below.

  •• **Military Capabilities Assessment.** Determining the adversary's potential military capability includes the identification of forces and dispositions, an evaluation of the adversary's

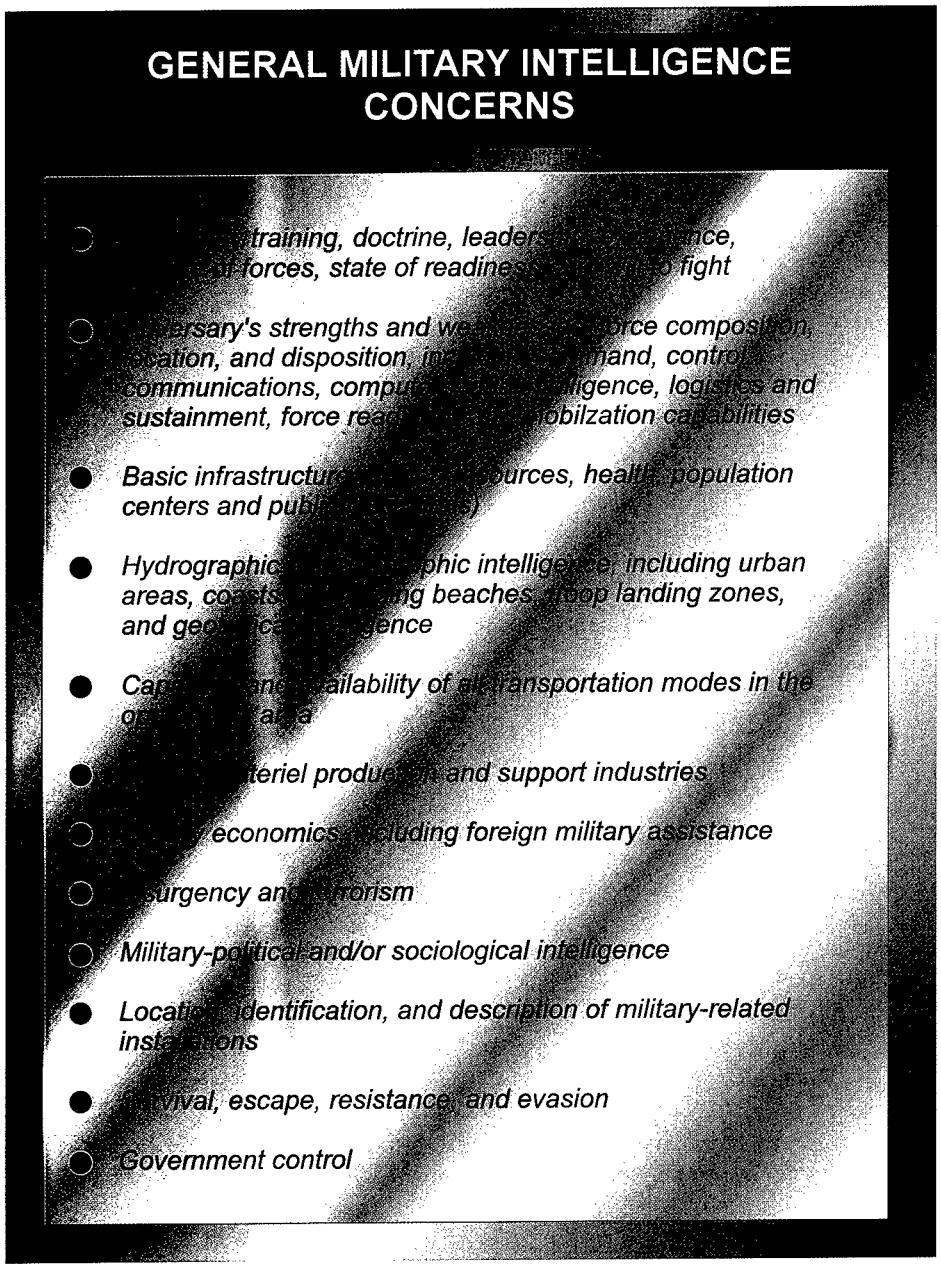
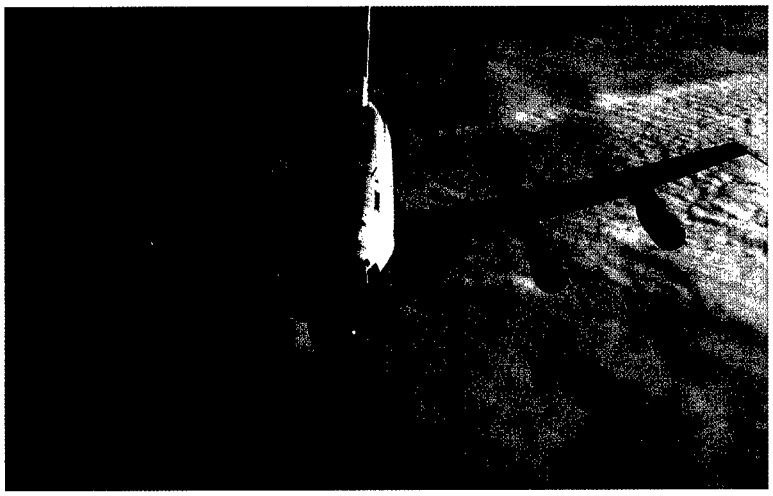


Figure III-18. General Military Intelligence Concerns

vulnerabilities, and an assessment of the adversary's ability to employ military force to counter the objectives of friendly forces. **The combatant command JIC is the subordinate joint force's primary source for all types of military capabilities assessments.** Subordinate joint force components continuously provide information to the joint force JISE to update military capabilities data bases. The five major components of an opposing force addressed in the assessment are as follows: (1) **Leadership and Command and**

Control (C2). An assessment of the adversary's ability to direct forces to accomplish a designated mission. Includes information on C2 nodes, lines of authority and reporting chains, and biographical data on key personnel. (2) **Order of Battle.** Identifies force components and assesses the strengths, structures, and dispositions of the personnel and equipment of the opposing military force, to include weapons of mass destruction. (3) **Force Readiness and Mission.** Assesses the adversary's readiness, as well as the doctrine it would follow and strategy and tactics it would employ, to achieve its objectives. (4) **Force Sustainability.** Assesses the ability of the force to logistically maintain the level and duration of combat activity (i.e., industrial, transportation and military infrastructure, supply status, attrition rates, and the adversary's morale) necessary to achieve objectives. (5) **Technical Intelligence.** Assesses the technical sophistication of forces, units, and weapon systems, as well as their capabilities, constraints, vulnerabilities, and countermeasures.

•• **Military-Related Subjects Assessment.** This type of assessment can **provide indicators of an opposing force's capabilities and vulnerabilities**, including its warfighting sustainability. Examples are as follows: (1) **C4 Systems.** An assessment of the adversary's C4 systems (i.e., telecommunications nodes and networks) to determine availability, connectivity, and vulnerabilities. (2) **Defense Industries.** An assessment of industrial production capacity, available stockpiles of goods and raw materials, natural resources, and reconstitution capability. (3) **Energy.** A listing of power sources and distribution network locations and capabilities. (4) **Military Geography.** A study of the impact that geographic features may have on planned operations, force deployment, and movement within the JOA. (5) **Demography.** Understanding the dispersion and cultural composition of the population (i.e., language, religion, socio-economic status, and nationality or ethnic groups) in the JOA critical to the nature of the operations to be conducted. (6) **Transportation.** The



The subordinate joint force J-2's first priority is to provide intelligence concerning the adversary.

lines of communications (i.e., location and capacities of airports, ports, and harbors; types, locations and capacities of roads, bridges, railways, and waterways) and equipment required by military, civil-military related activities. (7) **Environmental Considerations.** Oil dumping, ignition of oil field fires; diseases and health threats, such as contaminated areas and availability of water supplies; and other environmental factors that could affect military operations. (The combatant command JIC is the primary source for the latest intelligence assessments of environmental considerations.) (8) **Medical.** Availability of medical facilities, equipment, and supplies as well as professional medical personnel to treat casualties. Preventive medicine efforts, their effectiveness and impact on force readiness should be assessed. (The subordinate joint force itself and the combatant command JIC are the primary sources of information in support of these assessments.) (9) **METOC Support to Military Operations.** Climatology and METOC patterns that could affect friendly and adversary military operations. Understanding the opposing force's ability to assess METOC data is important in how the adversary may plan and conduct operations. (The combatant command JIC and the Joint METOC Operations Center or designated theater METOC unit are primary sources for assessing climatology and METOC patterns and the adversary's METOC capabilities.)

•• **Multidisciplined CI.** Multidisciplined CI threat analysis evaluates all foreign intelligence and security services disciplines, terrorism, foreign-directed sabotage and related security threats. Analysis focuses on the JFC's ability to sustain forward operations and protect lines of communications and main supply routes. Multidisciplined CI analysis includes detailed input to JIPB.

•• **Intelligence Estimate.** Once a basic understanding of the threat and pertinent military-related subjects has been gained, **it is necessary to try to view the situation through the adversary's eyes,** visualize which COA are available to the adversary, analyze the advantages and disadvantages of each from the adversary's perspective, and estimate which is the most likely option to be chosen. The joint force JISE and the combatant command JIC are the primary sources of information in support of these estimates.

•• **Intelligence Support to Military Operations.** The subordinate joint force J-2's first priority is to satisfy warfighters' requirements. **The J-2 should provide intelligence concerning the adversary and the environment needed by the JFC for determining objectives, selecting options, planning and conducting operations, and evaluating the effects of operations.** The subordinate joint force J-2 should fuse information from the combatant command JIC with subordinate joint force components' event-by-event reporting obtained during contact with opposing forces into a timely, coherent product describing how the operation is unfolding and providing an estimate of what actions the adversary will likely take in the following 48-96 hours. Longer term estimates should be made when practicable.

CI Threat Estimates and/or Vulnerability Assessments identify friendly weaknesses and vulnerabilities that may be exploited by an adversary. A personalities, organizations, installations and incidents data base provides indications to the motivations and ideology of those who may come into contact with or influence the joint force's operational area. Investigative reports provide insight into potential weaknesses. A commander can request and use CI information to protect personnel, equipment, and facilities.

d. **Target Intelligence. All-source analysis provides comprehensive targeting intelligence required for the commander to achieve operational objectives.** Targeting intelligence includes fixed and moving target signatures. Targeting production requirements include the following:

- Adversary means, methods, goals, options, objectives, strengths, weaknesses, values, and critical nodes.
- Target threat characteristics and vulnerabilities.
- Adversary centers of gravity.
- Analysis of information warfare and other non-lethal weapons.
- Precise target location information and target signatures.

The target intelligence package (TIP) is developed by the theater JIC. TIPs contain timely, detailed, tailored, and focused multi-source information describing the target; the climate, geography, or hydrography; the demographic, cultural, political, and social features of the operations area; and the threat, to include strategy and force disposition of military, paramilitary, or other indigenous forces and security or police forces of danger to US elements. The TIP must also contain current imagery of the target and JOA as well as accurate Geospatial Information and Services (GI&S) products.

e. **Scientific and Technical Intelligence. S&TI looks at foreign scientific and technical developments that have warfare potential.** This includes medical capabilities and weapon system characteristics, capabilities, vulnerabilities, limitations, and effectiveness, research and development activities related to those systems, and related manufacturing information.

25. Support to Combatant Commands

a. Combatant command, Service, and Defense agency production centers will provide the Defense Intelligence Production Functional Manager with periodic status reports on their respective center's capability to meet assigned tasks. Production-related responsibilities of combatant command J-2s (Figure III-19) include the following:

- To serve as overall shared production program (SPP) managers for their respective production center.
- To identify, consolidate, and validate command intelligence requirements for which intelligence production must be satisfied by maintenance and entry of data in SPP or command automated data bases.
- To participate in production program reviews and other forums.

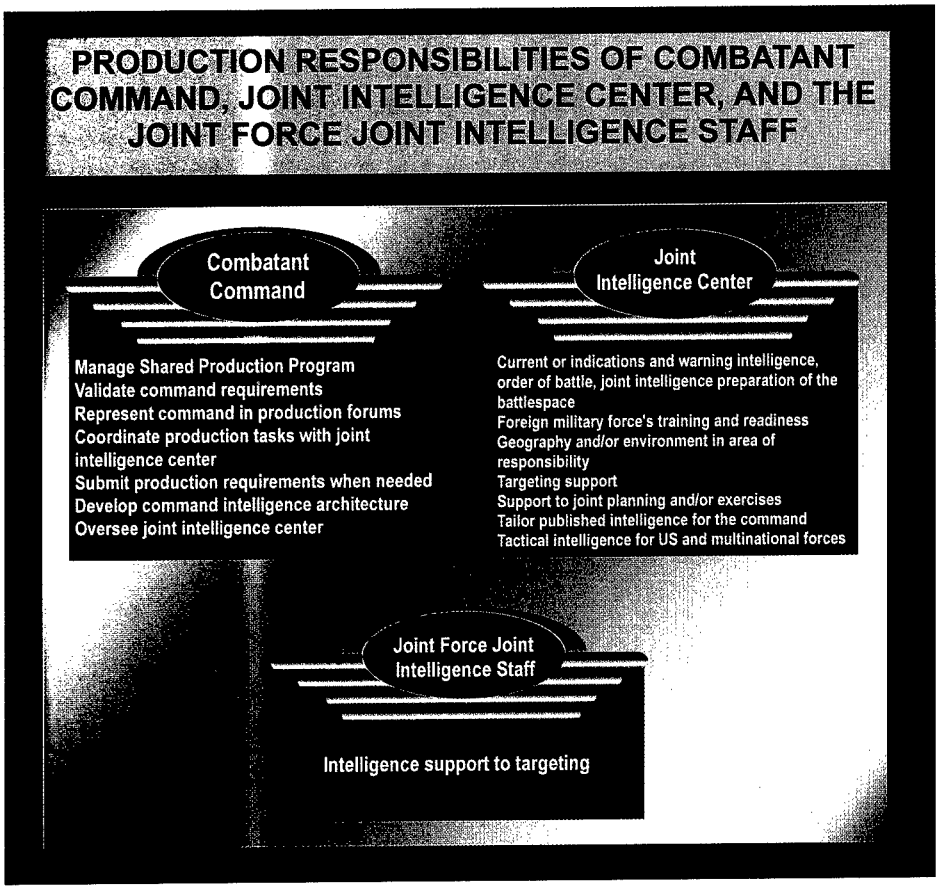


Figure III-19. Production Responsibilities of Combatant Command, Joint Intelligence Center, and the Joint Force Joint Intelligence Staff

- To coordinate the tasking and assignment of production responsibilities to the production center within the command's chain of command. For areas outside the theater JIC capabilities and responsibilities, forward a request for production to the appropriate command, Service or DIA.

- To develop command architectures with the necessary capacity, connectivity, and processing power to host, manipulate, and exchange intelligence required to support command operations.

- To oversee activities of the command production center to ensure provision of timely, accurate intelligence to theater consumers and/or operators.

- To deconflict production requirement priorities.

b. A combatant command's **intelligence production is performed by a production center, or JIC**, which is assigned directly to the combatant command in support of theater or specialized forces. The JICs are the cornerstones for fulfilling the intelligence requirements of the geographic combatant commanders and their subordinate commanders. The JICs provides tailored, finished intelligence products in support of theater mission planning and execution.

Production-related responsibilities of the JIC include analysis and production of the following:

- Current and/or I&W intelligence for forces deployed in the command's AOR.
- Potential adversaries' OB and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of those forces.
- Foreign military forces' unit-level training and/or operational readiness.
- Physical environment information (including development of terrain analysis products) in areas of potential operations.
- JIPB in support of joint operation planning and ongoing operations.
- Target support, including development of target materials, battle damage assessment (BDA), and SOF targeting support.
- Information to support command-sponsored joint planning and exercises.
- Predeployment support and tailored intelligence produced elsewhere to meet the specific requirements of the command's customers.
- Background and tactical intelligence for customers within the theater, including US and multinational forces.

c. Detailed intelligence is a critical requirement for conducting targeting. **Responsibility for targeting resides with the JFC.** However, JFCs normally will delegate the authority to conduct execution planning, coordination, and deconfliction associated with targeting and will ensure that the process is also a joint effort involving applicable subordinate commands. **The JFC's guidance directs and focuses operation planning and targeting to support the concept of operation.** The joint force J-2 is responsible for intelligence support to targeting. The targeting process selects targets (geographical areas, installations, activities or facilities planned for capture, disruption or destruction by military forces) and matches the appropriate response to them, taking into account operational requirements and capabilities. Targeting entails the analysis of adversary situations relative to the mission objectives. A detailed description of joint procedures for intelligence support to targeting is found in Joint Pub 2-01.1, "Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting."

d. **Combat assessment (CA) is the determination of the overall effectiveness of force employment during military operations.** Intelligence production support for CA includes detailed assessments of damage to the adversary's combat capability, summaries of adversary actions, predictions of adversary intent, and recommendations for future operations. The J-3, with input from component commanders and the J-2, has primary responsibility for CA. During the planning and execution of joint operations, a critical responsibility of the J-2 is to accumulate, consolidate, and report battle damage inflicted on the adversary as a result of combat operations. Timely and accurate BDA is a primary driver of combat operations. BDA incorporates assessments of physical, functional, and target system damage. The JFC requires continuous feedback on the status of mission objectives, and operators need BDA input to determine the relative success of completed attacks, the necessity and timing of restrikes, and the selection of follow-on targets. More information on CA can be found in Joint Pub 2-01.1, "Joint Doctrine, Tactics, Techniques, and Procedures for Intelligence Support to Targeting."

e. **IW targets information, information-based processes, and information systems.** The information system components consist of human factors, links and nodes. Offensive IW attacks an adversary's information infrastructure, erodes confidence in the information it provides, and enables commanders to operate within the adversary's decision making cycle. Defensive IW protects the friendly information systems, maintains confidence in its ability to support operations, and shortens decision cycles. **C2W employs various techniques and technologies to attack or protect a specific target set - C2.** DIA and the national S&TI centers provide technical analytical support and parametric data base information to the combatant commands in a variety of recurring and ad hoc documents and reports. Combatant commanders, subordinate component commanders, and JFCs plan and execute IW/C2W.

26. Production Responsibilities

a. **Production centers at all levels are assigned clearly delineated areas of analytical responsibility across the range of military operations.** These centers support the efficient use of production community resources, prevent duplication of effort, and provide timely support to customer requirements. The production community includes all DOD military intelligence production and activities except for NSA.

b. **The DODIPP is structured to capitalize on the analytical and production resources of the entire DOD Intelligence Production Community (DODIPC)** to focus expertise and maximize output to the consumer. The structure is an explicit, logical division of activities, responsibilities, and accountability among national, Service, and combatant command production centers, and by the national-level military intelligence forums. SPP structure and procedures facilitate central management and decentralized execution of defense intelligence production. SPP is described more fully in Appendix F, "Shared Production Program."

c. **The combatant command J-2s identify and validate command operational requirements.** The command's production center (JIC) schedules and accomplishes production activities for the theater, focusing on producing tailored, finished intelligence in support of theater mission planning and execution.

d. At the subordinate joint force level, production focuses on the fusion of all-source intelligence from components, the combatant command JIC, and national sources to support the joint force mission and operations. The combatant command JIC receives information from all echelons and performs all-source analysis and production. It is the primary source from which subordinate joint forces receive intelligence and intelligence products on their areas of interest.

e. **Lower echelons request, or pull, the tailored intelligence products they need from intelligence data bases electronically available at intelligence centers at all levels.** This concept allows joint force commanders to acquire relevant intelligence, based on their mission and the specific phase of the ongoing operation, using intelligence data bases physically maintained at other echelons and locations. The combatant command J-2 remains responsible for the coordination of intelligence information in-theater and manages the flow of intelligence through direct communication with each command and Service. The push and pull concepts are discussed further in Section E.

27. Request Management

a. Customers communicate requirements to their supporting intelligence office, an

existing military element or individual that serves DODIPC customers, which articulates the customers' needs as an RFI. **RFIs state questions the customer wants answered or contain other specific intelligence needs**, such as countries and topics required, in data bases, target materials, and hardcopy or other production media. RFIs also specify the various levels of detail required as well as the periodicity of production and updates. An RFI template is contained within the Community On-Line Intelligence System for End-Users and Managers (COLISEUM). COLISEUM automates the DODIPP procedures for registration and assignment of RFIs and subsequent tracking of the RFI.

b. After the supporting intelligence office surveys local resources and completed or scheduled production for duplication, it completes the PR in accordance with DOD-0000-151C-YR, "Department of Defense Intelligence Production Program: Production Procedures (U)," and submits the PR to the validation office (VO) at the next level in the Service, combatant command, or DIA chain. The DIA Directorate for Intelligence Production (DI), each Service, and each combatant command has a VO to process and validate the PRs submitted by their organizations' supporting intelligence offices.

c. Upon validation, the VO assigns production responsibility for the PR based on DOD-0000-151A-YR, "Department of Defense Intelligence Production Program: Production Responsibilities (U)." The VO transmits the assigned PR to a primary production center and information copies to possible collaborating production centers. Simultaneously, an information copy is sent to the Defense Intelligence Production Functional Manager (Director, DI).

d. **Once requirements are assigned to a primary production center, the center coordinates the efforts of all collaborating production centers for the designated product.** All centers schedule the production of each PR consistent with other assigned projects and DODIPP priorities contained in DOD-0000-151B-YR, "Department of Defense Production Program: Production Priorities (U)." The commander and/or director of each production center is responsible for submitting a binding, for-the-record assessment of the center's ability to respond to each PR.

e. After coordination with collaborating centers, the primary production office provides a written interim response to the customer, stating the format and type of document it will produce and citing a final response date. Copies of the response are sent simultaneously to the assigning VO(s), the collaborating production centers, and the Defense Intelligence Production Functional Manager.

28. Prioritizing Requirements

a. **All peacetime, crisis, and wartime requirements must be identified, documented, and prioritized.** Whenever possible, customer requirements should be satisfied with either existing intelligence products or modifications to existing products to prevent duplication of effort. Intelligence products must be in a format that the customer can understand and apply.

b. **The subordinate joint force J-2 is the focus for all intelligence requirements generated within the joint force staffs and/or at lower echelons.** These requirements are satisfied by the joint force J-2 through information the J-2 holds or can access via data bases, or that can be acquired by organic collection assets. If internally generated requirements cannot be satisfied by the subordinate joint force, the J-2 must pass them to the combatant command JIC through a controlled flow of RFIs. This includes RFIs that can be satisfied only by national agencies

and which may become PRs, before being forwarded from the combatant command. The subordinate joint force J-2 validates and prioritizes these requirements, along with those of the subordinate joint force, and submits them as a request to the combatant command JIC. When the combatant command JIC cannot satisfy these RFIs, it will forward them directly to the NMJIC. **Once RFIs and/or PRs have been submitted and accepted at any echelon, collection action is initiated as necessary.** While the status of the RFI/PR is managed at each echelon, the subordinate joint force J-2 is responsible for tracking the status of joint force and component RFIs and ensuring feedback to components on their requirements. (Figure III-20)

29. Evaluation

The production process is evaluated based on customer satisfaction with the product provided in response to a request. Intelligence personnel at all levels evaluate the production process and the products in an effort to continuously improve support to the requester. Evaluation includes the transition from the processing and exploitation phase, meeting production standards, improving processes, and customer feedback.

30. Additional Information

For additional information on intelligence production, see Joint Pub 2-0, "Joint Doctrine

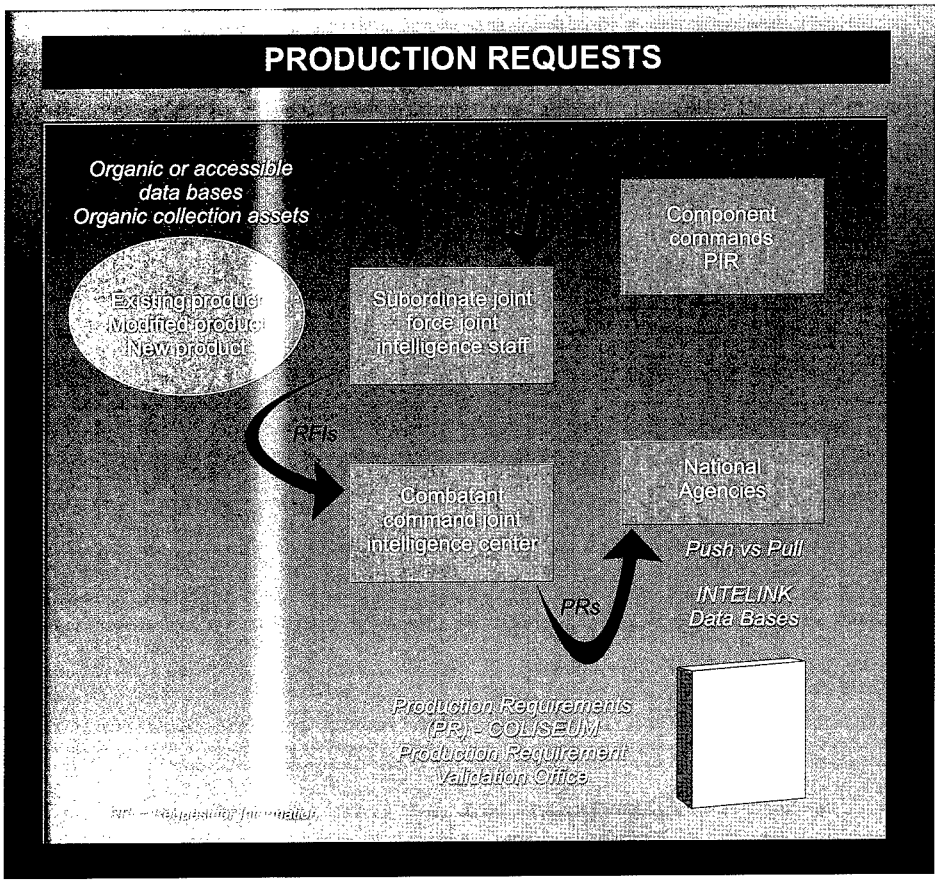


Figure III-20. Production Requests

for Intelligence Support to Operations" and DOD-0000-151-YR, "Department of Defense Intelligence Production Program."

SECTION E. DISSEMINATION AND EVALUATION

31. Overview

a. The J-2, at each echelon, manages the dissemination of intelligence to the user. **Intelligence must be provided in a form that is readily understood and directly usable by the recipient in a timely manner without overloading the user and, at the same time, minimizing the load on communications capabilities.** It is also important to provide for maximum possible release of appropriate classified reporting, analysis, and targeting data to multinational forces.

b. **Dissemination consists of both "push" and "pull" control principles.** (Figure III-21) **The "push" concept allows the higher echelons to push intelligence down to satisfy existing lower echelon requirements or to relay other relevant information to the lower level.** This includes warning data initially received only at the national or theater level; other critical, previously unanticipated material affecting joint operations; intelligence which satisfies standing information requirements by a subordinate unit; or specially prepared studies requested in advance by the subordinate joint force J-2. The push concept is managed

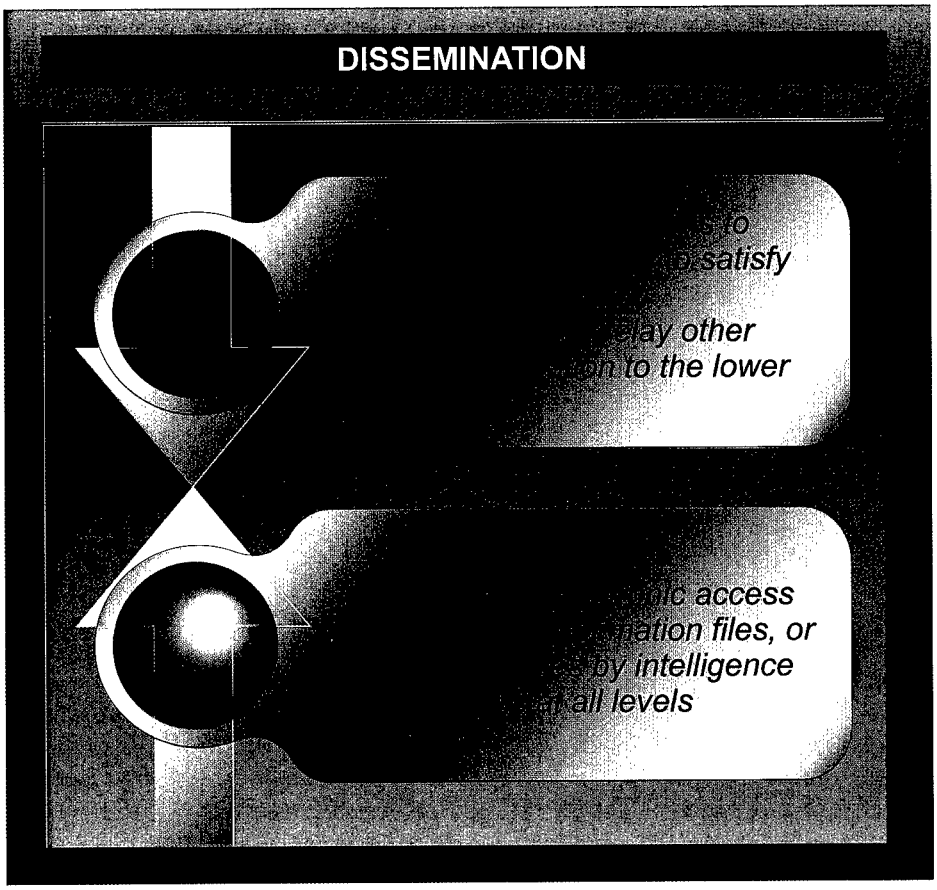


Figure III-21. Dissemination

through the Defense Intelligence Dissemination System (DIDS). DIDS contains the intelligence consumer's SII. When a producer wants to push an intelligence product to the consumer, they query the DIDS data base and create a distribution list. **The "pull" concept involves direct electronic access to data bases, intelligence files, or other repositories by intelligence organizations at all levels.** An increasing number of intelligence pull products are available on INTELINK or INTELINK-S (collateral version), INTELINK-C (Commonwealth version), INTELINK-P (Policynet), and other national and theater file servers. **The pull method is far quicker, and more preferred, than RFI/PR submission**, provided the desired information already exists in a usable form. However, a judicious push may be needed to avoid overloading the lower, support headquarters. The Global Broadcast Service (GBS) also provides a greatly enhanced capability to distribute multiple kinds of data, including bandwidth intensive video and imagery, to all levels of command.

c. During operation planning, the J-2 will coordinate with the J-3, J-4, J-5, J-6 and component commanders to ensure that specific transportation assets, personnel, equipment (especially communications) and procedures (e.g., in-theater courier aircraft, vehicles, liaison teams, networked intelligence workstations, facsimile [fax], voice, and other procedures) are available for disseminating intelligence and intelligence products within the AOR and/or JOA. The J-2's involvement during campaign and operation planning ensures his understanding of the intelligence products needed, required timeliness, consumer locations, and logistics and infrastructure assets available to support intelligence dissemination. This is particularly important during conditions of MOOTW when air, ground, and sea assets may be limited and lines of communications (LOCs) extended.

d. **A key to operational success is the timely and accurate dissemination of intelligence to deployed units.** The dissemination manager manages the dissemination of intelligence products to the user. A dissemination program manager (DPM) works with the dissemination systems to get the product to the user. Dissemination managers, in cooperation with the combatant command's DPM, must ensure that appropriate mailing addresses, Automatic Digital Network (AUTODIN) message addresses and routing indicators, and Special Security Office (SSO) security accreditation are requested and established for those units. This administrative information must be communicated to and validated by the command DPM, who will provide the information to DIA and other supporting national agencies. Further, the subordinate joint force J-2 should coordinate communications requirements with the joint force J-6 during the planning phase of the operation. (Figure III-22)

32. Dissemination Methods

a. **Hardcopy Dissemination.** Modern dissemination systems have overcome many historic dissemination problems. However, **the capability to deliver intelligence by fax, message, or courier in hardcopy remains a requirement**. In any operation involving allied or coalition forces, this is especially true as US intelligence equipment and system architectures are often not compatible or at the same security level.

- Combatant commands manage the movement of hardcopy intelligence to deployed subordinate joint forces in coordination with the J-3, the command logistics staff, the DPM, and the dissemination manager. Past operations and communication limitations associated with transmitting large format and/or color products have validated the continuing requirement to ship some

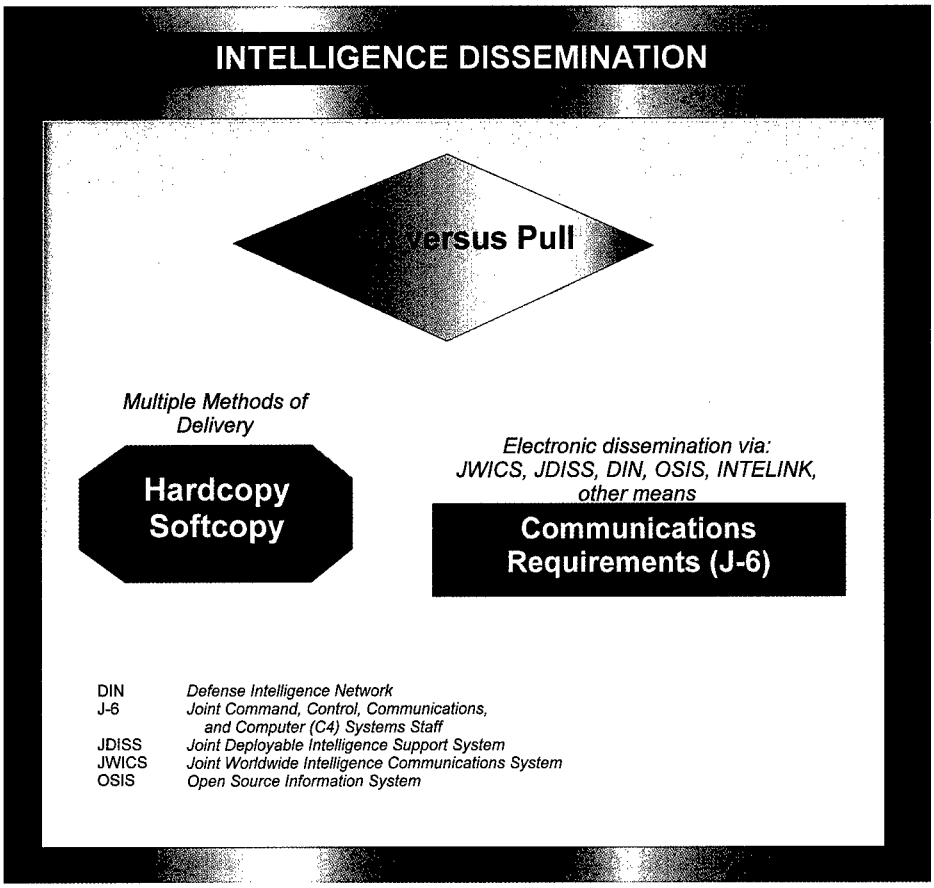


Figure III-22. Intelligence Dissemination

critical hardcopy products, such as basic target graphics, to consumers.

- From the beginning of any operation, the combatant command, or subordinate joint force J-2(s), establishes a dedicated procedure for moving hardcopy intelligence from the production centers to the theater and distributing it within the AOR and/or JOA. This includes nominating priorities to the JFC relative to available air and/or sea lift resources for delivery of hardcopy intelligence support products.

b. **Softcopy Dissemination**

- **An increasing number of intelligence community products are prepared in electronic form and are candidates for softcopy dissemination.** Publication producers and consumers are transitioning toward an all electronic product environment to improve the timeliness of intelligence dissemination and to reduce the amount of hardcopy distribution required. Reporting and archiving using electronic methods increase the intelligence community's capability to use electronic means to deliver intelligence to operational forces. With the advent of the communications tools Joint Worldwide Intelligence Communications System (JWICS), Joint Deployable Intelligence Support System (JDISS), Defense Intelligence Network, Open Source Information System (OSIS), Global

Command and Control System (GCCS), INTELINK and/or INTELINK-S, Integrated Broadcast Service via the GBS communications pipe, and GBS, dissemination capabilities are being expanded to deliver intelligence whenever and wherever adequate communications can be extended.

- JWICS or other sites that have electronic publishing capability and sensitive compartmented information (SCI) connectivity can pull electronic products. **INTELINK is the intelligence community architecture for sharing and disseminating intelligence**, allowing organizations to have the ability to produce their own documents or contribute (collaborative publishing) to the creation of other documents throughout the electronic publishing community. Once a user accesses the electronic publishing application, options would be available to view and index, access help menus, scan images, or open standard format templates. Standards are being established for file formats, naming conventions, directories, software applications, and graphic applications.

- Each J-2 site routinely has access to several daily current intelligence documents, including the Military Intelligence Digest, the NMJIC Executive Highlights, and Defense Intelligence Reports. Other documents (current and finished intelligence) as well as intelligence information reports and imagery are also being posted to servers (e.g., INTELINK, OSIS - unclassified only) for access by the combatant commands and subordinate joint forces. Other softcopy products include messages and intelligence data bases maintained by national-level agencies or theater JICs.

- Electronic documents dissemination media varies (e.g., softcopy, compact disk-read only memory [CD-ROM]), depending on the requirements of the end user. For example, JICs with INTELINK dissemination capability can pass the finished intelligence documents to their subordinate sites and/or create tailored intelligence products using CD-ROM or electronic publishing technology.

- **Much of the material on INTELINK is available to anyone with access to an INTELINK terminal.** With many documents already located on INTELINK, it may only be necessary for a site to tell the requester where the document exits. Requests for other existing electronic documents should be made directly via INTELINK or, if not directly accessible, pass the request to the appropriate DPM to satisfy the request. The softcopy document will in turn be placed either on the dissemination server for requester pull or electronic push.

- The Services and combatant commands are integrating softcopy dissemination technologies into their intelligence architectures. The subordinate joint force J-2 should quickly assess the equipment assets and training levels of all assigned forces to ensure timely dissemination of intelligence to all users.

33. Integration of Intelligence Products

The requester must integrate all intelligence obtained from national, theater, or organic resources and/or assets into the decision making and planning processes. The subordinate joint force J-2 is responsible for this integration process, updating the situation assessment and advising the JFC on any changes to the COA available to the adversary.

34. Evaluation

The intelligence dissemination and integration process needs to be continuously evaluated. Intelligence personnel at all levels assess the success of the dissemination and integration phase of the intelligence cycle and make changes as needed to improve the process. The evaluation looks at the transition from the production phase and into the next iteration of the intelligence cycle; the achievement of dissemination standards; performance improvements of both personnel and the process; and customer feedback.

Intentionally Blank

CHAPTER IV
INTELLIGENCE C4 SYSTEMS SUPPORT

"The success of any crisis deployment hinges on the existence of a reliable command and control system and of a flexible, reliable system for gathering, analyzing, and disseminating strategic and tactical intelligence."

General H. Norman Schwarzkopf, USA, USCINCCENT, Operation DESERT STORM, 1991

1. Introduction

a. **Communications and automated data processing (ADP) systems provide the basic framework for the timely movement and transfer of intelligence in each phase of the intelligence cycle to commanders and other key decision makers.** Communications and ADP technology is undergoing continuous evolution, affecting intelligence architecture, systems, and applications. This presents challenges regarding operator familiarization, integration and compatibility of systems, and efficient utilization of available resources. These challenges can be overcome through dedicated, professional training and hands-on experience.

b. Developers, installers, and other ADP professionals must continuously raise the threshold of dynamic support to commanders by successfully creating and refining communications and ADP systems. **However, integral to all system development and application is the need for utility** — technology is not an end in itself, but the means to process and pass intelligence in support of the commander and the mission. Technological development must be realistically tempered by the limitations of fielded and deployed systems and of the consumers themselves.

2. Intelligence Communications Capabilities

a. **Joint Intelligence.** Joint intelligence architecture **implements common procedures, standards, and streamlined support**, and continues to evolve in concert with the Command, Control, Communications, Computers, and Intelligence (C4I) for the Warrior Concept. This broadly connected joint system provides total battlespace information to the warrior, and establishes a global C4I capability for the warfighter to "plug in" anytime, anywhere, for any mission. (Figure IV-1)

b. **National Agency Communications Support.** As discussed in Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations," **the Director, DIA, establishes capability and interoperability standards for joint and Service intelligence activities.** The Director coordinates planning and programming of intelligence resources, including those for selected ADP systems, telecommunications, and survivability. DIA has established a standard communications architecture that supports joint intelligence operations. The geographic combatant command then takes this standard "package" and, in coordination with DIA, builds a theater intelligence architecture based on the mission, CINC guidance, and command requirements.

3. Multinational Force Intelligence and Communications Interoperability

a. Multinational operations are now the norm for military operations, making intelligence-sharing with the allies

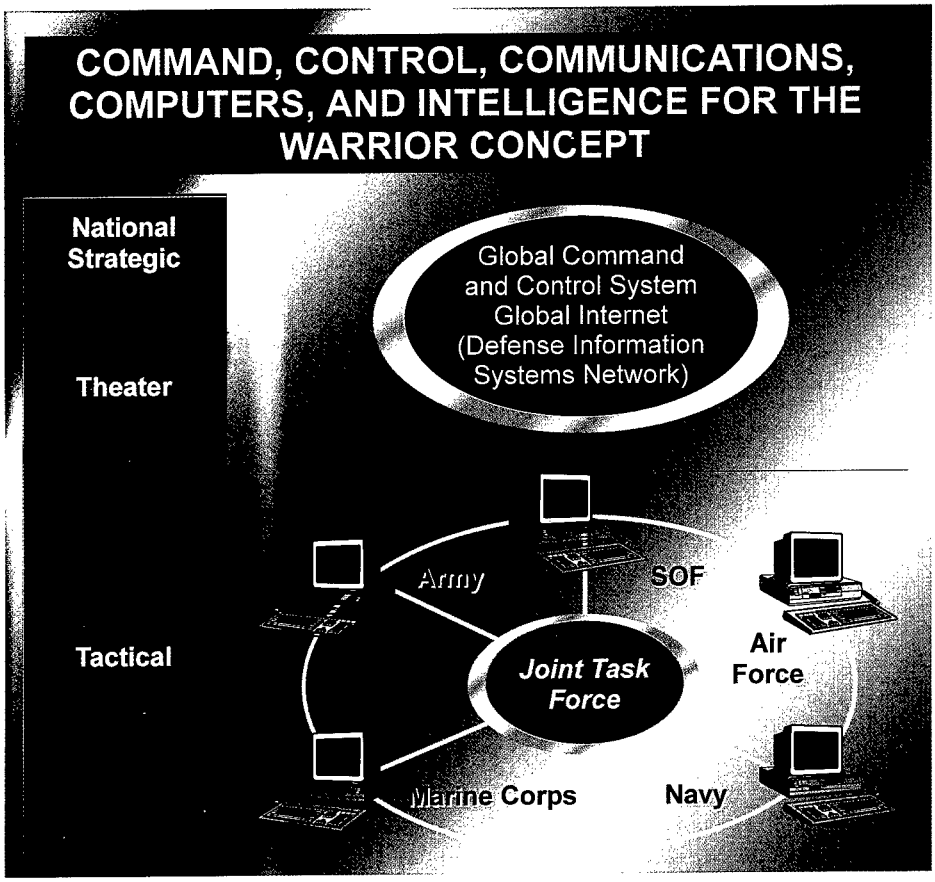


Figure IV-1. Command, Control, Communications, Computers, and Intelligence for the Warrior Concept

increasingly important. **A multilevel security system does not currently exist that can easily facilitate sanitization and dissemination of intelligence to US and allied and/or coalition operational commanders.** Combatant commands and subordinate joint task forces can request that intelligence reports be made releasable to coalition and/or allied nations as necessary. INTELINK, available on JDISS, provides some uniform methods and tools for exchanging intelligence.

b. **A subordinate joint force should be interoperable with, and have access to, theater-ADP systems and data bases**, as well as allied and/or coalition force and component command systems such as Linked Operational Intelligence Centers Europe (LOCE). LOCE is the primary automated system for exchanging intelligence with NATO allies. A similar interoperability exists in Korea with the Pacific ADP Server Site-Korea.

4. Establishing Intelligence Communication Systems Requirements

a. A wide range of national, theater, and component intelligence and communication systems are available to a JFC. The continuing evolution of the primary Department of Defense Intelligence Information System (DODIIS), including the JWICS and the JDISS or client-server environment (CSE)

compliant workstation, enables the design and implementation of a robust and flexible capability for a subordinate joint force. The existence of this capability does not, however, ensure that intelligence and communications systems can be deployed without significant planning and coordination. Supporting communications paths will probably have to be procured or extended to link the JFC with the Defense Information Systems Network (DISN). **The theater J-2 must understand current systems sufficiently to tailor an architecture integrating intelligence sensors, processors, dissemination systems, data bases, and ADP and communications systems.** The J-2 needs to maximize the use of the in-theater communication resources and then deploy ancillary equipment to extend the communications links from the DISN to the warfighter. Since the preferred equipment or communications paths may not be available for a quick reaction to a contingency, alternative systems and/or subsystems and communications paths may have to be used or procured. The subordinate joint force J-2 must effectively coordinate communications architecture requirements with the J-6 and coordinate with the J-4 and other logistics elements for the timely delivery and installation of intelligence and communications systems. In addition, communications systems requirements for national-level connectivity for NIST support should be forwarded to Joint Staff J-2 for validation and tasking. The combatant command or the joint force J-6 should coordinate with the NIST for their communications planning and support. Interoperability problems need to be addressed and resolved during the planning phase.

b. **Key concepts to successful intelligence systems support are joint interoperability, streamlined flow of information, and providing pull-down of intelligence tailored to the needs of the operating forces.** The ability to provide the tactical commander with real/near real time intelligence continues to be a critical factor. (Figure IV-2)

- In planning a communications architecture, **step 1 includes identifying the type of mission, the concept of operations, joint and Service doctrine, and the specific mission requirements.** Step 1 functions are developed to meet specific mission objectives of the JFC and each of the subordinate commanders and an operational scenario for the mission. Step 1 products include lists of the subordinate joint force composition and the assets assigned from national, theater, and Service levels, and a specific activity timeline for operations planned by the JFC and each subordinate commander.

- In **step 2 the specific communication intelligence support plan for the joint force is determined by the mission and the intelligence support concept** developed by the component commanders in the theater of operation. This model identifies the intelligence functions required to support the subordinate joint force commander and the intelligence information flows required to support each function.

- **Step 3 compiles the intelligence information flows from step 2 into a node-to-node layout of intelligence information transactions.** Nodes are used to represent the headquarters and the external supported and/or supporting organizations. This is done by numbering the nodes of interest and developing needlines. A needline represents the flow from one node to another.

- **During step 4 the joint force J-6 staff will determine the communications support plan** for requirements identified in step 3. The requirements developed by the J-2 planning staff can either be analyzed separately or combined with similar inputs from the J-1, J-3, J-4, J-5 and J-6 staffs at each security level.

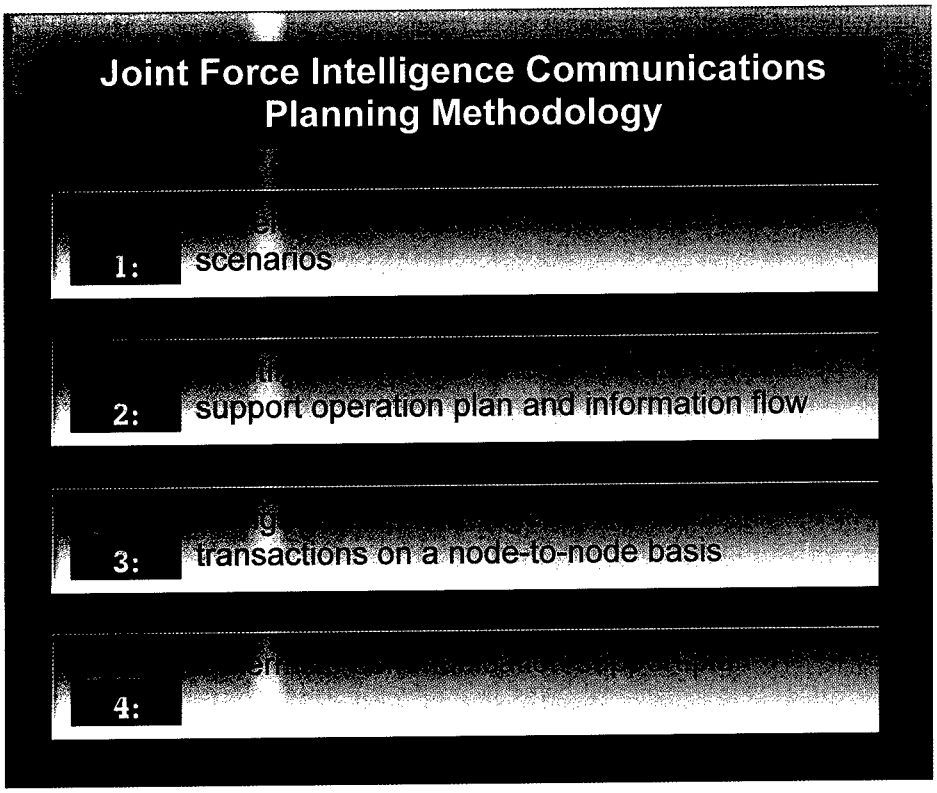


Figure IV-2. Joint Force Intelligence Communications Planning Methodology

5. Combatant Commander's Communications Planning

a. **Architecture Planning**

- In the past, planning for external subordinate joint force exchanges was accomplished by multiple organizations, resulting in redundant communications. Interoperability was hindered by a lack of governing architecture, resulting in dissemination requirements not being satisfied. CINCs planned their connectivity to the subordinate joint force, and the national intelligence agencies planned their connectivity to the NIST at the subordinate joint force. These requirements should be planned collectively prior to operational deployment rather than independently, thus ensuring that an integrated communications support plan is developed for the subordinate joint force(s).

- **The combatant command J-2 and J-6 should set up adequate communications paths for the JFC** and/or subordinate joint force intelligence needs prior to operational deployment. (Figure IV-3) The joint force should use established wide area networks as the basis for planning its communications, ADP support, and dissemination to the joint force component commanders at the Top Secret and/or SCI and Secret levels. **In coordination with the J-6, the J-2 builds a tailored, integrated architecture that incorporates sensors, processors, and dissemination systems with ADP and communications systems** (e.g., JWICS). This architecture links the subordinate joint force with the Service components and coalition or allied units

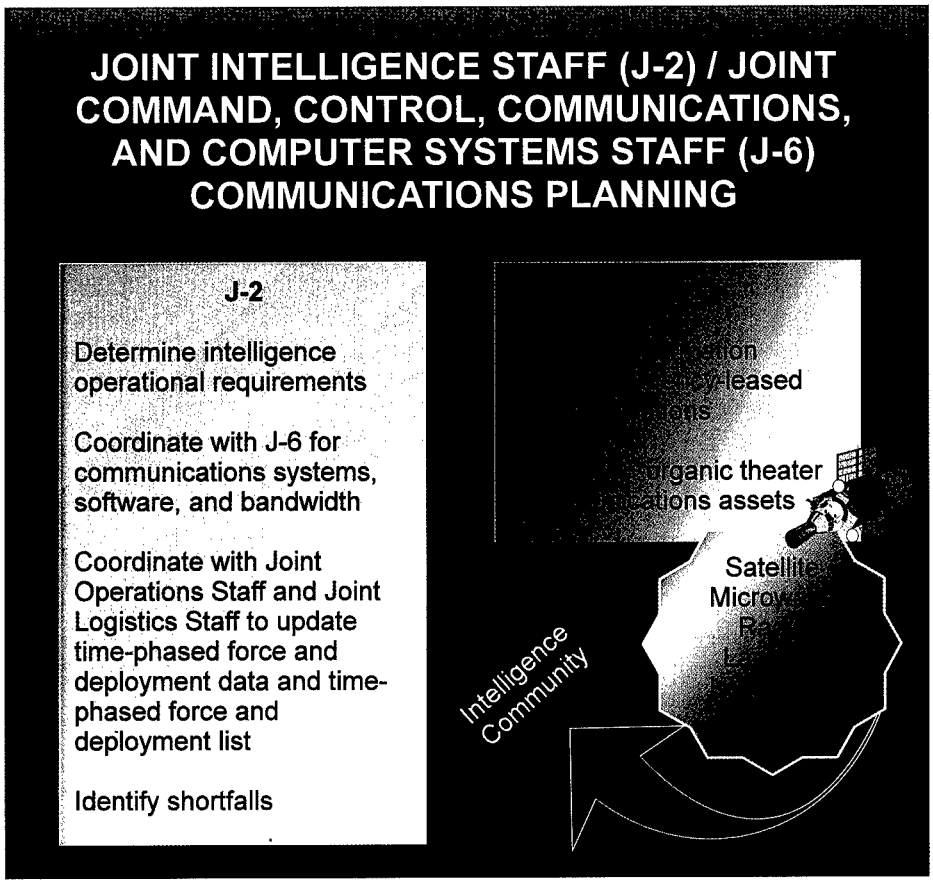


Figure IV-3. Joint Intelligence Staff (J-2)/Joint Command, Control, Communications, and Computer Systems Staff (J-6) Communications Planning

as well as with the combatant commands and the NMJIC. The major components of the joint intelligence architecture provide connectivity between the joint force and the national and component levels. This tailored architecture includes prototype equipment and units with different or unique systems. Once the architecture is defined, the J-2 works with the J-3 and J-4 to update the TPFDD and TPFDL. The J-2 and J-6 should solve any interoperability problems prior to resource deployment.

b. **System Planning**

- **Organic communications asset requirements must be identified to the J-6.** As soon as the subordinate joint force J-2 determines operational and dissemination requirements, the J-2 requests support from the subordinate joint force J-6 for the necessary communications systems, communications security (COMSEC), application software, and communications bandwidth needed to provide simultaneous transmission of secure, interactive video teleconferencing; dissemination of selected products using graphics, desktop publishing, data, and secondary imagery; and secure voice. Shortfalls in communications support are identified and submitted to higher headquarters for resolution.

- **Subordinate joint force communications links include satellite, microwave, radio, landline, and local area networks (LANs).** The subordinate joint force J-2 and J-6 identify the proper frequencies, communications protocols (bit rate, parity, and other communications protocols), network security management requirements, encryption devices, and procedures for the architecture components. The resulting communications capability interfaces with the global intelligence infrastructure, i.e., the national intelligence community, the combatant command JIC, the subordinate joint force and components, and allies and/or coalition partners.

- **Requests to the combatant command J-6 for DISA-leased or non-organic theater communications resources may become complex.** For example, if requesting a wide-area network (WAN) service such as DISN, JWICS, or GCCS, the subordinate joint force will likely need Joint Staff and DISA coordination and DIA and/or NSA requirement validation. The J-6 requires detailed information for formal request documentation. **Special provisions exist to expedite service under emergency conditions**, including telephonic requests followed by confirming documentation within 48 hours. Information required includes the type of telecommunications support required, proposed location, time required to be operational, duration, funding and justification. For a circuit requirement, the request should indicate terminal types at all locations; estimated intelligence traffic volumes; precedence and security levels; types of available encryption; (common-user or sole-user); specific locations; point-of-contact; any recommended restoration priority; usage duration; and type of circuit special considerations. The subordinate joint force prepares a telecommunications request for service and submits it to the appropriate command or J-6 validating authority. This process can be completed in advance by establishing contingency or on-call circuitry activation in accordance with an approved OPLAN.

- The standard tactical entry point (STEP) makes this process easier, using existing Defense Satellite Communication System strategic earth terminals to provide warfighters with a standardized set of pre-positioned circuits for entry into the DISN. STEP serves as a C4I communications hub to maximize satellite resource efficiency and access to services.

c. **Planning Considerations**

- Joint intelligence is rapidly evolving and testing "pull down" concepts. **The "pull" concept allows JFCs to acquire relevant intelligence when needed**, based on their mission and the specific phase of the ongoing operation, using intelligence data bases physically located and maintained at various locations. The theater JIC should determine the location of the desired intelligence and push the necessary information directly to all echelons requiring that intelligence in order to control the intelligence flow.

- **Every subordinate joint force operation requires planning for the exchange of intelligence within a deployed joint force and between the deployed joint force and supporting intelligence organizations.** Intra-subordinate joint force communications should support the exchange of situation data, RFIs, intelligence, and tasking of organic collection resources among the major elements of the deployed joint force and supporting intelligence organizations worldwide. These exchanges include the following:

•• **Intelligence exchanges within and between each Service and functional component assigned or attached to the subordinate joint force.** Each Service and functional component should deploy with an organic tactical communications capability that meets intra-Service exchange requirements. However, this capability may not support exchange requirements to other Service components' subordinate joint force elements.

•• **Exchanges between the headquarters of the subordinate joint force and, if designated, the headquarters of the Service and functional components.** Any intra-subordinate joint force requirements for intelligence exchanges at lower echelons can either be routed through these headquarters or identified as special requirements that must be planned separately.

•• **Connectivity requirements of the JFC to the combatant commander and to the national intelligence support agencies** (e.g., connectivity for the NIST that may deploy to support the JFC), to other supporting commanders and, in special cases, to other subordinate joint forces.

•• **Connectivity requirements from the assigned components to Service intelligence centers** in theater and the continental United States (CONUS) must also be addressed.

- The requirement to exchange large quantities of perishable data among dispersed forces places special demands on many communications networks. Additionally, the planner must understand the possible adverse effect large volumes of intelligence data may have on a limited bandwidth transmission system. **Communications systems do not have an infinite capacity.** Joint Pub 6-0, "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations," states: "Combatant commanders will determine the priorities of C4 systems and allocate communications circuits and channels (bandwidth) within the geographic or functional area of responsibility of their commands, including those required by component and other subordinate commands."

- **Required communications capabilities** considered by J-6 and J-2 planners **includes channel capacity**, defined as the maximum rate at which information can be sent over a communication channel without error. Imagery transmission requirements are of particular concern because of their high bandwidth requirements, which are directly proportional to the degree of resolution desired (i.e., the higher the resolution, the longer the transmission time via a given bandwidth). The J-6 and J-2 planners must ensure that high bandwidth transmissions such as imagery do not preclude or delay the receipt of other transmissions (e.g., messages), affecting the operation. Wideband circuits required to resolve this problem are costly and not always available in tactical locations. While satellite transmission systems offer high volume and broad coverage (compared to landline and line of sight radio systems), overall transmission capacity is limited to the radio frequency spectrum. Landline system capacity is limited by the amount of wire or fiber in place throughout the system.

6. Communications and Intelligence Systems

The joint intelligence architecture encompasses both the JWICS and the

A SIGNALMAN'S ODYSSEY

In January 1946, 4 months out of Japanese prison camp, Technical Sergeant Michael Maslak arrived at Arlington Hall Station—headquarters of the Second Signal Service Battalion. The battalion, along with its worldwide detachments, had played an instrumental role in helping to secure the Allies' victory over Japan. The young soldier brought with him a most adventurous story. The following is one facet of that story.

"The first radio intelligence (RI) job [in the Philippines] was the intercept of three types of communications: transmissions from and to the Japanese reconnaissance planes which were frequently observed; traffic of the air-ferrying commands in the Philippines area; and reports from Japanese weather stations scattered about the islands.

Our setup was makeshift, of course. Our antennas were outside and reached the receivers via a very long lead-in. For receivers, we had two Super-Pros—all we could ask for in the way of reception and as many as the initial four of us could man. All of us did intercept, but Lieutenant Brown and Lieutenant Gelb also had to evaluate the traffic and make translations (there was much plain-text), coordinate our results with G-2, and perform liaison. We were also in direct telephone contact with the Navy, which had an RI setup in the Navy tunnel near Monkey Point. A naval officer helped us a great deal in plain-text translations.

When the Japanese bombers started using radiotelephone, we obtained two interpreters, a Filipino and a Japanese-American to read the enemy's voice transmissions for us. The Japanese-American, despite his being highly trusted, could go about only under the guard of an American officer, lest he be mistaken for an enemy.

We knew the transmitting frequencies of almost all the air bases from which planes came over. The type of traffic they sent was always the tip-off of an impending raid. Special frequencies were used for bombing; they alone were an invaluable source of intelligence for us. We came to know planes' call signs by heart as well as the pilots' nicknames or codenames; they would use information as to their intentions, but they also kept us well informed of their results. They would report their losses and casualties, bombing or observation outcome, and what US batteries got the planes that were shot down, etc. They would then attempt to knock out the US batteries responsible for inflicting the damage."

SOURCE: Michael Maslak, *Signalman's Odyssey*
Military Intelligence: Its Heroes and Legends, compiled by Diane L. Hamm
US Army Intelligence and Security Command History Office, October 1987

JDISS and other CSE compliant workstations and strives to enhance joint interoperability by using common procedures, standards and streamlined support to provide intelligence to joint commands. (Figure IV-4)

a. **Joint Worldwide Intelligence Communications System.** A JWICS containerized and mobile capability has been developed to support contingency requirements through the use of military or commercial satellite or terrestrial earth terminals. The containerized JWICS is designed with six containers of video and communications gateway equipment. **The mobile JWICS system is the JWICS Mobile Integrated Communications System (JMICS).** JMICS provides a scaleable, deployable JWICS that is self-contained on a heavy high mobility multipurpose wheeled vehicle for rapid deployment in all-weather, austere environments. Key features include satellite connectivity, facsimile, collateral and SCI LAN-capable workstations, JDISS network servers, capability for two simultaneous video teleconference sessions, T-1, TROJAN Special Purpose Intelligence Remote Integrated Terminal II or commercial interface, and other key features. The Joint Staff J-2-controlled JWICS will be deployed in support of NIST or joint force requirements as well as other CJCS missions.

- **JWICS is a smart multiplexer-based, secure (Top Secret and/or SCI), high**

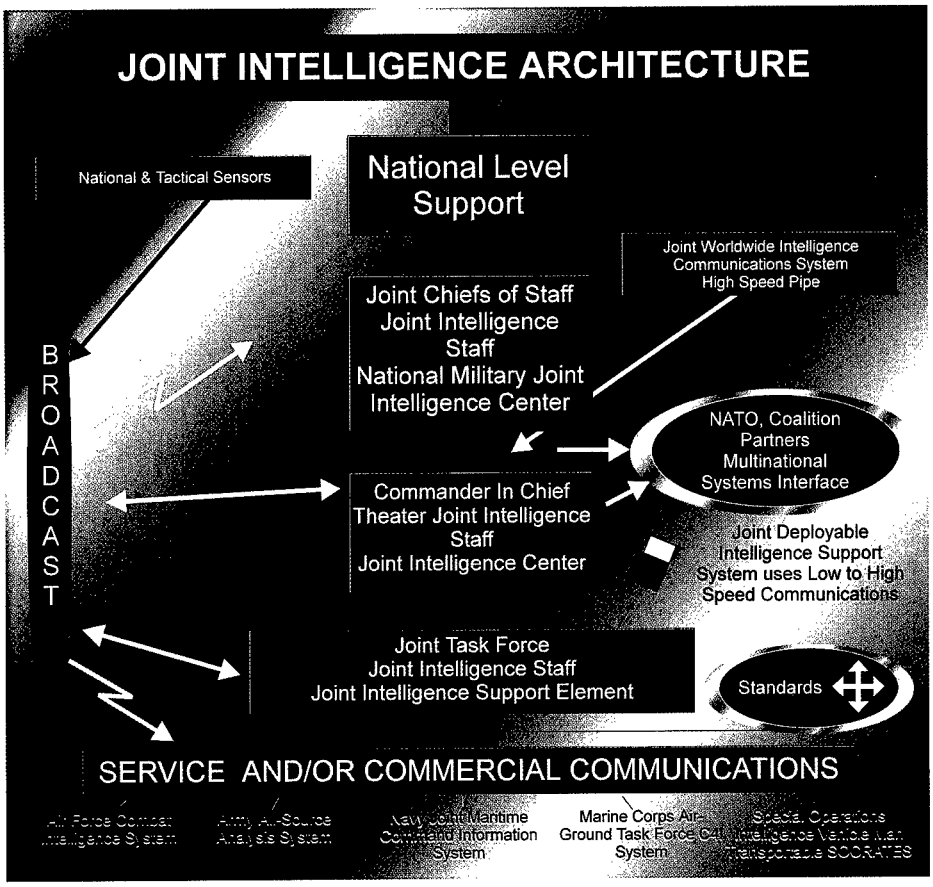


Figure IV-4. Joint Intelligence Architecture

speed multimedia intelligence communications network designed to support intelligence production and dissemination as well as crisis management operations. JWICS meets the requirements for dedicated, interactive, and high bandwidth video-capable communications for the Defense intelligence community. JWICS serves the NCA, Joint Staff, combat support agencies, all combatant command JICs and components, the Service intelligence departments, scientific and technical intelligence production centers, and selected military and civilian Federal executive agencies. Further, JWICS connectivity has been extended to deployed land-based and afloat sites as part of the NIST crisis contingency support concept for regional military operations.

- **The strategic objective of JWICS is to provide for interoperable, seamless, and responsive intelligence communications connectivity** for the military intelligence community to support operations. This effort has included the development of JWICS in three modes, i.e., fixed, containerized, and mobile, with the capability of supporting a joint force or NIST in a building and/or field site.

- The complementary architecture of JWICS (data and/or video) and JDISS workstations (data) spans national, operational, and tactical levels. **The major JWICS applications are: electronic publishing; video teleconferencing; bulk data transfer, including very large-file imagery; and video telecasting** such as the defense intelligence network (DIN). The DIN uses JWICS technology to accomplish live, broadcast dissemination of the latest intelligence developments worldwide.

b. **Joint Deployable Intelligence Support System. JDISS bundles commercial off-the-shelf hardware and software applications in a standard desktop environment.** JDISS provides a field-deployable office automation suite built upon the system security infrastructure provided by client-server environment system services. JDISS also allows electronic mail and chatter between intelligence echelons via the site's existing communications architecture. JDISS provides access to theater, Service, and national intelligence resources, such as data bases, basic imagery analysis and dissemination capabilities, specific analytical tools, and support functions required to execute the intelligence mission. JDISS is the preferred method of providing secondary imagery dissemination to the combatant commanders and subordinate JFCs. JDISS interfaces with GCCS.

c. **INTELINK. INTELINK is a principal electronic means for intelligence product dissemination.** INTELINK builds on ongoing architectural initiatives at the Top Secret and/or SCI and Secret and Unclassified classification levels. (Figure IV-5) INTELINK provides a comprehensive set of tools to query, access, and retrieve information. INTELINK permits collaboration among policy developers, analysts, and users, and will simplify access to a wide variety of services. The J-2 should assess the availability of INTELINK access among assigned and en route forces. The J-2 should also ensure that users have adequate system training and are aware of available products, content, and access procedures.

7. Communications and ADP Systems and Networks

The "Communications Handbook for Intelligence Planners (U)" and Joint Pub 6-02, "Joint Doctrine for Employment of

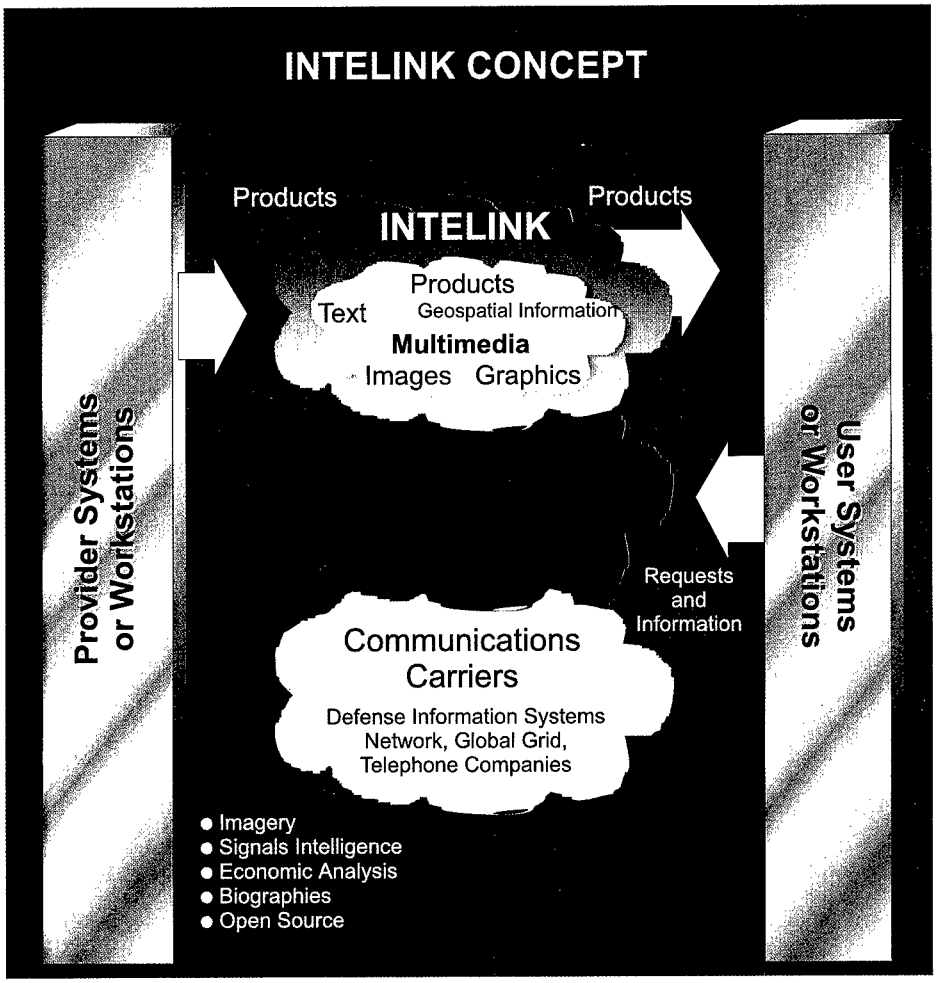


Figure IV-5. INTELINK Concept

Operational/Tactical Command, Control, Communications, and Computer Systems" provides more information on the systems briefly described below.

a. **Automatic Digital Network is an automatic store-and-forward message switching network** which provides hardcopy and softcopy message dissemination to users. The Defense Message System, which operates on the strategic and tactical level, will replace AUTODIN and other message-handling systems. It is designed to interface with the commercial and allied message and data systems.

b. **Department of Defense Intelligence Information System is the intelligence component of the DISN**, the DOD telecommunications infrastructure that supports military operations. DODIIS defines the standards for intelligence system and application interoperability. The DODIIS concept provides, within limits, an integrated strategic and tactical user environment for performing identical intelligence support functions on compatible systems. DODIIS provides a robust and flexible intelligence capability for the subordinate joint force as long as supporting communications lines are available. DODIIS tools support the

movement of intelligence between DIA, the combatant commands, the Services, and other intelligence production and customer activities worldwide. This program includes hardcopy products, digital or "softcopy" products, on-line access to data bases, the ability to "push" or "pull" files of information between producers and countries, CD-ROM storage, document imaging, electronic publishing, and networked (via internal LANs or JWICS) corporate mass storage devices to contain large volumes of digitized intelligence information. Figure IV-6 identifies the DODIIS information architecture.

c. **The SECRET Internet Protocol Router Network (SIPRNET) is the Secret-level WAN**, with a worldwide backbone router system. Various DOD router services and systems are migrating onto the SIPRNET backbone router network to serve the long-haul transport needs of the users. This network supports national defense C4I requirements.

d. **Global Command and Control System**

- GCCS is being implemented in accordance with the C4I for the Warrior concept. **GCCS is a highly mobile, deployable C2 system that supports forces for joint and combined operations** throughout the range of military operations anytime and anywhere in the world with compatible, interoperable, and integrated C4I systems. GCCS incorporates policies,

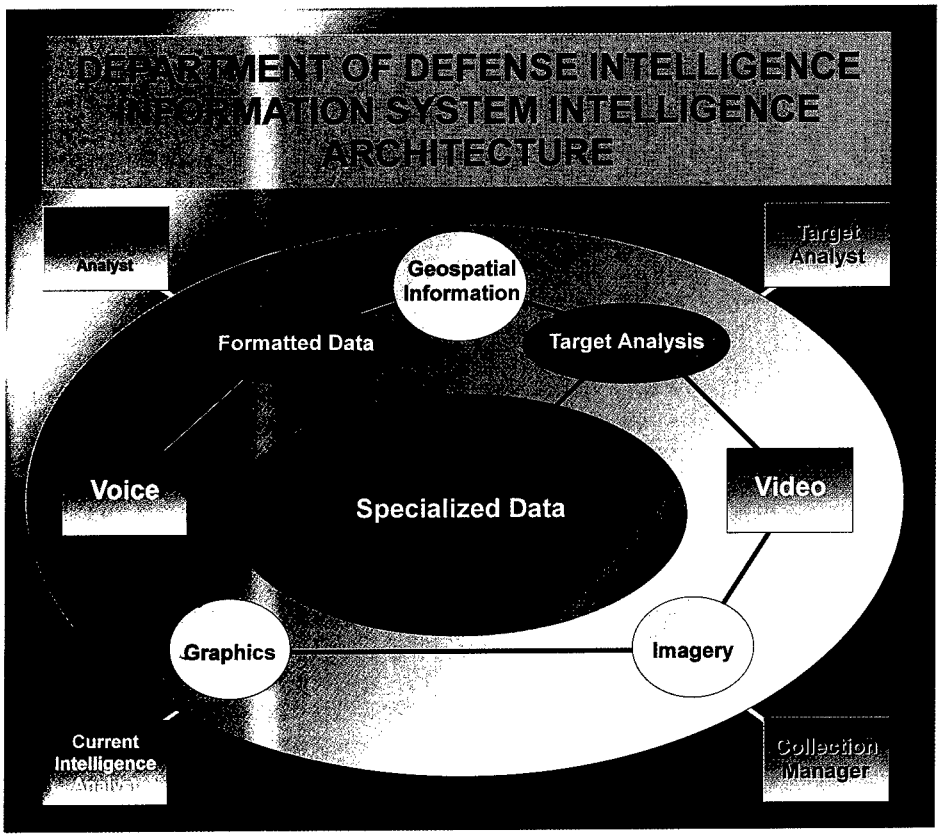


Figure IV-6. Department of Defense Intelligence Information System Intelligence Architecture

procedures, reporting structures, trained personnel, automated information processing systems, and connectivity to provide up to Secret-based information necessary to plan, deploy, employ, and sustain forces.

- GCCS meets the C2 requirements of the NCA through the subordinate joint force by encompassing four main communities: National (NCA, the NSC, CJCS, and Service Headquarters); Theater (supported CINCs and their component commanders); the subordinate JFCs and their component commanders; and supporting groups (supporting CINCs and their component commanders, Service major commands, combat support agencies, UN and allied commands, and other US government agencies such as the Department of Transportation [the US Coast Guard], the Drug Enforcement Administration, the Federal Emergency Management Agency, the Federal Bureau of Investigation, and the Department of State). The system provides analytical tools, information processing technologies, and real time information across an array of functions that will enable CINCs and subordinate JFCs to monitor operations in support of ongoing military operations. The system depicts a fused, near real time, true representation of the battlespace. At all user levels, the system normally provides information on a pull basis, so that the user can tailor information requirements. Push updates automatically distribute critical changes to ensure that the operator receives current information and intelligence. The intent is to meet multiple users' requirements by providing concise information tailored to the users' needs on a single system that eliminates multiple platform displays.

Global Command and Control System supports joint and combined forces and is highly mobile and deployable.

e. **GBS is an information service that uses commercially developed direct broadcast technology** to provide a wide range of information, including intelligence and intelligence products, to the warfighter. This simplex broadcast system is initially using leased commercial satellite capacity to provide high bandwidth capacity for broadcast of information such as imagery, video, environmental data, logistics, and warning to all command levels.

f. **Migration Defense Intelligence Threat Data System (MDITDS) provides**

an automated environment in support of threat analysis and warning for DOD commands, services and agencies. MDITDS tracks and/or assesses capabilities, intentions, methods and operations of countries, groups, organizations and individuals who pose a threat to US interests. Specific production within MDITDS includes counterterrorism, CI, weapons proliferation I&W, and defense industries. The MDITDS automated environment includes a single entry to review a variety of government and commercial information sources and provides the consumer with the ability to manipulate, analyze, produce, coordinate and disseminate intelligence and warning products.

g. **Military Intelligence Integrated Data System/Integrated Data Base (MIIDS/IDB)** provides sets of data elements and the capability to relate items of intelligence information with other items within the data base itself; for example, relating OB information to installations. The Modernized Integrated Data Base replaces the MIIDS/IDB.

h. **Joint Collection Management Tools (JCMT) provides the collection manager with an automated means of tasking national and theater collection resources and/or assets in support of operations.** Rapidly accessible data bases allow the user to review resource and/or asset capabilities, ensure efficient tasking of those resources, and track the status of the tasking. JCMT supports CRM through the use of platform and target area coverage along with timelines for planned missions. System functions include resource and/or asset capability and availability analysis, message processing of over thirty message types and/or formats, full-duplex accredited communications, data base management of and interactive operation with over twenty data bases (target, contact, references, and symbology), and system security administration.

i. **Requirements Management System (RMS) provides the national and DOD imagery communities with a uniform automated collection requirements management system.** Further information on RMS is available in Appendix C, "Intelligence Disciplines."

j. **The Joint Communications Support Element (JCSE).** The JCSE is a unique communications organization. JCSE provides contingency and crisis communications to meet the operational and support needs of the JCS, Services, combatant commands, Defense agencies and non-Defense agencies. Requests for support should be completed IAW CJCSI 6110.01, "CJCJ-Control Tactical Communications Assets." The JCSE provides tactical communications support for two simultaneously deployed subordinate joint forces and two joint special operations task forces. The JCSE possesses a wide range of communications capabilities tailored to meet a variety of contingency missions, including intelligence.

8. Other Communications Resources

a. **National Intelligence Support Team Communications Support Elements (NCSE).** The Chairman of the Joint Chiefs of Staff authorized the designation of existing intelligence communications units as NCSE to meet the need for timely communications connectivity between deployed NISTs and their national support infrastructure. These NCSE activities provide direct JWICS connectivity to the national support infrastructure. The NCSE activities operate under Joint Staff J-3 tasking as validated by Joint Staff J-2 in coordination with the Joint Staff J-6. The combatant command J-6 has the responsibility to provide frequencies for NIST satellite communications (SATCOM) activities. NCSE activities include the following:

- NSA/O55 maintains, issues, or deploys small fly-away NIST communications systems, including tri-band SATCOM, to support contingency or first-out NIST team needs. NSA/O55 also maintains, deploys, and operates light-sized transportable NIST communications systems including tri-band SATCOM, as well as medium-sized drive-away NIST communications systems, including redundant tri-band SATCOM in support of unique NIST or subordinate joint force requirements. All systems provide direct JWICS connectivity and include secure voice and data (JDISS) capability.

- The Army maintains, deploys, and operates TROJAN SPIRIT IIs and JMICS in support of joint requirements for intelligence support to subordinate joint forces and NIST. These systems provide up to 1.544 megabytes per second communications connectivity to support full JWICS, JDISS data, secure voice, and other unique intelligence communication needs.

b. Liaison with other agencies or Service elements with communications capabilities, such as NSA or a Public Affairs group, may reveal existing or available communications links in place. While these organizations have their own requirements, in a crisis the J-2 may arrange to temporarily share their circuits to meet critical needs.

Intentionally Blank

APPENDIX A
JOINT FORCE J-2 QUICK REACTION CHECKLIST

Overview

This checklist is an effort to assist a subordinate joint force J-2 and staff by providing a quick reference guide for a crisis situation. This is a guideline or point of departure, and should not be construed as all-inclusive. Depending upon the nature of the crisis (war or MOOTW), many of these variables may or may not apply. Other considerations not listed may also become factors.

ESTABLISH MISSIONS AND/OR TASKS

- Clarify and prioritize the subordinate joint force J-2's missions, tasks and requirements with input from the subordinate joint force J-3, and confirm with the subordinate JFC.

- Assist the J-3 in documenting intelligence requirements based on operational priorities and/or capabilities and mission requirements.

- Work with the J-3 in the development of mission objectives.

- Ensure distribution as appropriate, complete understanding of the tasking and guidance from the commander, and that it has been analyzed and applied to regional and/or theater assessments.

- Ensure that regularly updated intelligence collection and production priorities are passed throughout the entire chain of command, including components and supported commands.

- Determine theater intelligence architecture for flow of responsibilities for satisfying PIR, RFI/PR (i.e., theater intelligence assets). Intelligence responsibilities must be clearly delineated among subordinate joint force, combatant command, and national levels. Determine whether any subordinate joint force units (SOF in particular) require intelligence support from the combatant command or national level that the theater JIC cannot provide.

- Determine theater intelligence architecture for flow of secure communications, collection, dissemination, and ADP assets. Identify problems of coordination, interoperability of systems or supply and/or sensitivity issues.

- Determine status (number, type, readiness condition) of subordinate joint force's organic intelligence collection, production, exploitation, dissemination and communications assets.

- Conduct liaison, supervise, and coordinate other intelligence-related functions with appropriate staff elements and subordinate and supporting commands. Specific responsibilities include the following:

  •• IW, including C2W (J-3). Subsets of C2W are as follows: (1) Electronic warfare (EW) (J-3, or EW Officer when assigned). (2) Military deception (J-3). (3) Psychological operations, to include an estimate of conditions and vulnerabilities of prospective target groups; an estimate of the effectiveness of friendly and adversary psychological operations; and planning assistance and supervision of training activities concerning defense against adversary propaganda (J-3). (4) Operations security (J-3). (5) COMSEC (J-3/J-6),

communications electronics officer and/or NSA. (6) Information security program (J-6).

•• Counterintelligence (J-2 and/or CI).

•• Reconnaissance (J-3).

•• Counterterrorism (J-3).

•• Antiterrorism and/or force protection (J-3).

•• Handling of enemy prisoners of war (EPW), detainees, and captured documents and materiel (J-1/J-4).

•• Debriefing of EPW and refugees, exploitation of captured documents and equipment (J-2).

•• Transportation intelligence (USTRANSCOM/J-2).

•• Adversary employment of special weapons (nuclear, biological, and chemical [NBC]) (J-3 and/or NBC officer).

•• Combat assessment, to include BDA, munitions effectiveness assessment, and mission assessment (J-3).

•• Medical intelligence (Surgeon and/or DIA).

•• Civil affairs (J-3).

•• Barrier and denial operations (J-3).

•• Survival, evasion, resistance, and escape (J-3).

•• Language capabilities of subordinate joint force personnel (J-1).

•• Classified courier issues (J-1).

•• Geospatial Information and Services (GI&S Officer).

IDENTIFY SUPPORT NEEDED

- Intelligence Services and/or Products

  •• Identify available intelligence assets in-theater, including ADP systems and/or tools.

  •• Determine whether there is a requirement for Service, theater or national intelligence agency support, e.g., NIST, JWICS.

  •• If so, identify entities to be tasked and mix of skills and capabilities needed. Identify proper chain of command for requests.

- Personnel. Ensure that required and/or additional expertise is available, with sufficient personnel to meet watchstanding, courier, security and liaison requirements.

  •• Identify any requirements for personnel augmentation, to include regional or functional experts, linguists, and/or reservists (prior and/or advance joint training is a key factor for consideration).

  •• Determine augmentation support that can be obtained from theater assets. Coordinate tasking for those assets through the combatant commander's staff.

  •• Determine augmentation support that must be obtained from outside the theater. Coordinate with the J-1 as early as possible in the planning process to request support from external sources.

  •• Assume that the operation for which the subordinate joint force was

established will continue for an extended period of time, then make plans to request and accommodate rotation of staff and support elements and additional augmentation.

•• Identify any need for a deployable element to support the subordinate joint force's efforts in: collection management, HUMINT collection, Service expertise, communications, tactical or in-depth analysis, debriefing.

- Logistics

•• In concert with the combatant command J-2 and the subordinate joint force J-4, ensure that transportation requirements for high priority personnel and materiel are documented and prioritized. If this is an unforeseen contingency or crisis, there will not be a precut time-phased deployment plan for personnel and materiel, and the J-2 must assist the J-4 to ensure that intelligence needs are documented and met.

•• Ensure that transportation requirements for high priority intelligence personnel and or materiel are in concert with J-3 requirements. For example, target materials should be close to bombs in transportation priority if the former are to be of any use.

- GI&S Support. Shortfalls of critical GI&S products and digital data severely restrict the planning and analysis phases and may become a war stopper during the execution phase. No command can afford to conduct military operations with outdated or missing geospatial data for its forces or weapon systems.

•• Initiate single GI&S POC. Notify subordinate forces of correct requisition procedures for predeployment maps, charts, and digital data.

•• Notify combatant command GI&S staff of the GI&S support POC in the subordinate joint force.

•• Identify subordinate joint staff GI&S requirements to the combatant command GI&S staff with respect to forces deploying and the operational area. Include map production quantities, personnel and equipment to operate a map depot, and staff support personnel.

•• Request the following from the combatant command GI&S staff: the production schedule; status of products and digital data required and date of first shipment; status of host-nation support for GI&S products, digital data and capabilities; and the status on disclosure and/or release of geospatial information to coalition forces.

•• Verify and/or submit OPORD Annex M to J-2.

•• Request that supporting forces provide GI&S distribution plan. Ensure that combatant command and joint force GI&S staffs are provided a copy of all distribution plans.

•• Send message reminding forces about accuracies, datums, and coordinates of GI&S products and digital data.

•• Coordinate shipment of deployment stock to the map depot (unit line number). Obtain weight, cubic feet, number of 463L pallets and ready-for-shipment date from the combatant command GI&S staff. Forward unit line number to the combatant command GI&S staff.

•• Establish map depot inventory quantities to include reorder levels. Report results to the combatant command GI&S staff via AUTODIN message, electronic mail, or JDISS.

•• Request that the combatant command GI&S staff have DMA publish special operation catalog.

- METOC Support. METOC support can help optimize intelligence support in a variety of ways (assisting in collection management, helping to anticipate adversary actions). Coordinate with the Joint Force METOC Officer through the J-3, if applicable, for needed METOC products and services and for the transfer of METOC data received through intelligence resources that could supplement the METOC data base.

ESTABLISH A JISE

- Determine whether a JISE is required to support the subordinate joint force; establishment of a JISE will be theater and/or situation dependent.

- If a JISE is to be established, consider the following:

•• Facility location and physical security requirements.

•• Personnel requirements, including augmentation.

•• JISE structure requirements for: (1) Joint Captured Materiel Exploitation Center (JCMEC); (2) Joint Interrogation and Debriefing Center (JIDC); (3) Joint Document Exploitation Center; (JDEC) (4) Collection Management Section; (5) Intelligence Support Section; (6) Targeting Support and BDA Section; (7) Other intelligence production; (8) Communications and ADP support; (9) Soft-copy and/or electronic and hard-copy product dissemination to components; (10) Receipt, processing and exploitation of imagery and production of imagery-based materials; (11) Establishment of subordinate joint force JISE relationships and connectivity to component, combatant command, and national intelligence; (12) Supplies needed for a lengthy deployment, if a JISE or other intelligence element is forward deployed; (13) Security; and (14) Military deception.

- Develop intelligence communications architecture with reporting and requesting channels.

INTELLIGENCE COLLECTION MANAGEMENT

- In concert with the combatant command J-2 and the subordinate joint force J-3, ensure that all intelligence collection requirements are identified as early as possible.

- Develop and publish intelligence collection requirements. Establish time schedule for updates.

- Identify organic collection capabilities and status of all component and supporting units as well as those en route to the operational area.

- Identify any shortfalls in collection capabilities. Ensure that collection requirements to cover such shortfalls are developed and forwarded through the combatant command JIC to the NMJIC for subsequent national resource tasking.

- Ensure that collection activities are coordinated with the Defense Collection Coordination Center through the combatant command JIC and the NMJIC.

- HUMINT collection

•• Establish the need for a subordinate J-2X to manage, coordinate and deconflict HUMINT, CI, Country

Team and/or SOF collection activities. Coordinate with the combatant command J-2, HSE and CISO for requesting required resources from DHS and the Services and appointment of HOC and TFCICA.

•• Establish the need for a JIDC to satisfy subordinate joint force and combatant command PIR. Request staffing from the components and DHS, as required.

•• Establish the need for and request further HUMINT collection augmentation and support from DHS.

- IMINT collection

•• Obtain emergency dissemination authority for imagery and imagery products. Emergency dissemination authority is a powerful tool, designed to support military operations, including those involving allies.

•• Tailored imagery should be requested as soon as a target is identified. All imagery should be forwarded to requester.

•• Establish the need for and request further IMINT collection augmentation and support from the Services or national imagery agencies.

- SIGINT collection

•• Coordination of SIGINT support for JTF operations should be accomplished through the commands organic cryptologic support division in concert with the respective CSG and command NCR.

•• Establish the need for and request further SIGINT collection augmentation and support from the Services or NSA.

- All other intelligence disciplines.

INTELLIGENCE PRODUCTION MANAGEMENT

- Coordinate with theater JIC to determine whether PIR have already been established for current situation. PIR should be built around commander's requirements.

- As needed, in concert with J-3 and theater JIC, tailor PIR for current situation.

- Keep PIR current and update periodically.

- Develop or acquire a complete intelligence assessment of the situation.

•• Periodically update situation assessment.

•• Submit completed situation assessment to the commander and chain of command.

- Ensure regional and threat assessments are current.

- Ensure key friendly and neutral forces have been identified.

- Coordinate the theater and national assessments and provide copies to subordinates and components.

- Ensure all required intelligence annexes have been incorporated into the OPLAN or OPORD.

- Closely track intelligence collection and production requirements to completion.

C4 SUPPORT (FOR SUBORDINATE JOINT FORCE INTELLIGENCE)

- The J-2 should establish and maintain regular dialogue with the combatant command J-2 and the Service component

intelligence staff officers.

- Request JCSE support/augmentation.
- As soon as possible, coordinate with the J-6 to ensure communications lines are available.
- Know the capacity of communications paths serving the subordinate joint force, between the subordinate joint force and its components and with allied or coalition units.

  •• Assess the C4 capabilities and requirements of all assigned intelligence elements and those en route to the operational area.

  •• Intelligence exchange with allied and/or coalition units may require a liaison with secure portable communications and ADP support.

  •• Minimize. Keep communications paths open by eliminating extraneous traffic. Units with global missions routinely subscribe to numerous summaries from all theaters. Assign lowest possible precedence on summary messages. Cancel summaries for the subordinate joint force staff and components and rely on tailored support from the JIC.
- Fully apprise subordinate joint force and senior commanders of all relevant current events.
- Ensure subordinate joint force J-2s' ADP equipment is compatible with theater and subordinate systems. For coalition subordinate joint forces, ensure systems are compatible.
- Ensure communications lines have sufficient baud, rate capacity or bandwidth.
- If necessary, establish a tactical SCI facility (SCIF).
- Identify COMSEC and determine availability.
- Ensure all router tables are updated.
- Ensure all AUTODIN AIG are updated, complete and used.
- Eliminate duplicate data being disseminated to the same users by different means.
- Ensure ADP security measures are employed properly.
- Determine reporting/production times and types of reports.

MULTINATIONAL INTERACTION

- Establish liaison between joint and multinational force intelligence structures.
- Ensure procedures have been established and reviewed to expedite sanitization and sharing of US-generated intelligence products with allies.
- Ensure friendly objectives, intentions, and plans are fully communicated to appropriate intelligence organizations.
- Ensure interoperability of C4 systems.
- Be aware of, and remain sensitive to, cultural and/or religious differences among coalition members. In some instances, these may result in periods of increased vulnerability for the joint force, or may require scheduling changes for meetings and/or briefings.

CI/COUNTERTERRORISM

- In coordination with the J-3 and coalition intelligence and/or CI elements, develop and implement CI and counterterrorism plans to support requirements.
- The J-2 should appoint a TFCICA.
- Ensure CI is incorporated into planning as a force protection measure.
- Ensure CI is included in collection management planning.
- Advise component CI organizations and begin planning coordination with the Joint CI Support Branch and other combatant command CISOs for national-level joint CI assistance.
- Ensure intelligence security guidelines have been developed and disseminated.
- Ensure development and required approval of CI Force Protection Source Operations umbrella concept.

SECURITY

- Ensure personnel and information security measures, including those applying to ADP, are enforced throughout the joint force.
- Enforce need to know criteria for release of all information related to the operation.

Intentionally Blank

APPENDIX B
REPRESENTATIVE INTELLIGENCE REQUIREMENTS

Overview

An illustrative table of intelligence requirements is provided as a starting point for developing a mission specific list. This reflects the probable intelligence needs of a combatant commander. The list is representative of the major concerns of a commander at any level, but is not offered as a definitive, exhaustive compilation of every possible concern. A combatant command J-2 or subordinate joint force J-2 preparing PIR for the commander's approval can use this table to stimulate ideas and to identify information gaps, especially since different Service and/or functional components may require more detailed information than outlined in the intelligence requirements provided below. The mission-specific list should be prioritized to ensure that collection decisions can be made rationally and that the intelligence effort remains focused on responding to the most important requirements first.

INTELLIGENCE REQUIREMENTS

- **Assess Damage 1.** Assess impact of execution of psychological operations.
- **Assess Damage 2.** Assess extent of soft or hard damage to adversary combat units in order to plan restrike and follow-on phases of the operation.
- **Assess Damage 3.** Assess status and adversary ability to repair, reconstitute, recuperate, or relocate vital infrastructure, weapon systems and forces. Provide data which allows assessment of mission results against overall campaign objectives and tactics.
- **Assess Damage 4.** Determine which military units have sustained significant (30%) casualties.
- **Beach Defenses.** Determine adversary beach defenses; provide timely surveillance; locate and/or identify coastal defense units (priority on artillery, mechanized infantry, and armored units).
- **Casualties.** Predict number of friendly and adversary casualties and chemical, biological, or radiation injuries to estimate transportation, hospital space and medical support required.
- **Commercial Traffic 1.** Identify air, sea and ground commercial routing, traffic, and density within the operations area. Identify commercial air corridors.
- **Commercial Traffic 2.** Provide information on all shipping to include suspected carriers of contraband, major ports of debarkation, historic shipping density data, and daily operation summary of expected departures, arrivals, and schedules. Identify types of vessels.
- **Counterintelligence.** Describe country's awareness or knowledge of, and countermeasures to, US intelligence activities.
- **Combat Search and Rescue (CSAR) 1.** Identify survival, evasion, resistance, escape, and recovery procedures, and selected area for evasion (population characteristics; culture; location; approaches; contact recovery points and procedures; security hazards; cover and concealment).
- **Combat Search and Rescue 2.** Identify and locate allied and/or coalition partner personnel for rescue. Determine

adversary knowledge, reaction, or movement to CSAR operation area.

- **Demographics/Culture 1.** Identify languages, dialects, ethnic composition (both national and target area).

- **Demographics/Culture 2.** Describe customs (social, weapons, religious, cultural, mores).

- **Demographics/Culture 3.** Identify tensions (regional and national; causes, intensity, degree, and exploitability by the United States or opposition).

- **Demographics/Culture 4.** Identify foreign influences (sources, leaders, themes, influence on government, unions, students, insurgents and general public).

- **Demographics/Culture 5.** Characterize attitude of civilians and civilian groups to US involvement (friendly, unfriendly, or neutral), and for planned US operations (support, oppose, tolerate).

- **Demographics/Culture 6.** Estimate assistance available to US forces (extent and capabilities, laborers, linguists, liaison, analysts, administrators); determine attitude of neutral population toward host country, threat policies, and actions.

- **Demographics/Culture 7.** Determine probable reactions of leadership and population in country to US unconventional warfare or other SOF activities. Determine how country will treat those indigenous personnel who participated in wartime unconventional warfare or SOF activities in postconflict environment.

- **Demographics/Economics 1.** Assess civilian economy and war sustaining infrastructure; include community structures, industrial base and complexes, resources and strategic reserves, petroleum production, storage and/or distribution, weapons systems and/or munitions, research and development, stockpiles, electric power, and transportation.

- **Demographics/Economics 2.** Estimate available labor force (location, numbers, equipment, skills).

- **Demographics/Economics 3.** Assess effect of any UN and/or international sanctions on the country's ability to wage war.

- **Demographics/Economics 4.** Identify civilian supply shortages. List commodities available for potential use by US forces. Determine status of local food or market distribution system. Identify food stocks, stockpiles, and warehouses.

- **Demographics/Information 1.** Describe information or propaganda service, apparatus, or organization (key personnel, attitude toward the US Government, whether usable by US forces) and employment of propaganda and disinformation (current, future capabilities).

- **Demographics/Information 2.** Determine if military personnel have access to commercial radios and/or televisions; automated information management systems; type of printed material they carry, literacy rate, languages used. Provide samples.

- **Demographics/International 1.** Describe country diplomatic activity.

- **Demographics/International 2.** List membership in international organizations (UN) or groups (Red Cross).

- **Demographics/International 3.** Characterize human rights history (friendly and threat countries); and US policy toward country's human rights actions.

- **Demographics/International 4.** Describe country's government or popular support of regional insurgencies (groups, movements, type of support).

- **Demographics/International 5.** Identify foreign military or political agents of influence within country.

- **Demographics/Medical 1.** Determine the health threat to friendly forces. Describe local diseases, extreme environmental conditions, locally available illegal drugs, and flora and fauna which may contribute to the health threat.

- **Demographics/Medical 2.** Determine local public health facilities status and needs, to include level of staffing available; specific health services provided; health and sanitation conditions; major health-related problems; shortages of medicines, pharmaceuticals, or equipment including transportation.

- **Demographics/Miscellaneous.** Miscellaneous (including currency, holidays, dress, customs, and foreign influences).

- **Demographics/Political 1.** Opposition to existing US forces, facilities, or interests (general population and significant groups and forces).

- **Demographics/Political 2.** Describe adversary nation's political leadership structure and dynamics, with particular emphasis on command and control facilities. Describe country's political structures, parties, and leadership organizations.

- **Demographics/Political 3.** Describe country's internal groups (indigenous elements who are members, level of popular support, group's support or non-support of governing regime).

- **Demographics/Political 4.** Provide biographical sketches of all significant political leaders and advisors and military leaders down to division level (background, education, talents, connections, political affiliations, orientation, US training).

- **Demographics/Political 5.** Describe anti-government opposition groups or resistance forces (names, organization, leaders, political affiliation, size, support); military capabilities (organization, equipment, training, ability to conduct sabotage, subversion, deception); and communications.

- **Demographics/Political 6.** Determine threat to US personnel from opposition or resistance groups.

- **Demographics/Political 7.** Identify military or civilian leaders within potential insurgent groups who will support coalition efforts.

- **Demographics/Political 8.** Identify military or civilian leaders within potential insurgent groups who would make acceptable post-hostility leaders. Identify military and civilian leaders, whom, if protected, would enhance post-hostility restructuring.

- **Demographics/Political 9.** Assess vulnerabilities of objective country government to insurgent attack (prioritize).

- **Demographics/Political 10.** Identify US-provided materials or services urgently needed or required by cooperating indigenous military, paramilitary, resistance forces, or local nationals.

- **Demographics/Population.** Describe area population characteristics.

- **Demographics/Refugees.** Estimate number of dislocated civilians, disruption to civilian infrastructure, and refugee movement. Identify and locate camps and camp managers. Determine support requirements (shortages of food, medicine, shelter, clothing).

- **Demographics/Religion.** Describe key religions and impact on ethical or decision making processes. Identify key religious leaders, factions, and groups.

- **Demographics/Social Conditions 1.** Describe civil disturbance and riot control training (units and their capabilities).

- **Demographics/Social Conditions 2.** Determine status and needs of local public administration and law enforcement. Can local, regional, or national administrators continue essential functions? Identify key leaders of the various civil agencies or departments. Status of jails and prisons.

- **Demographics/Social Conditions 3.** Determine status and capability of power, telecommunications, water, sewage, refuse collection, fire-fighting, and public transportation services. Are facilities secured (by whom)? Identify capability to transport water (trailer, tanker). Is local water potable?

- **Environment.** Describe adversary intentions and capabilities to conduct environmental warfare (oil dumping, ignition of oil field fires, release of toxins).

- **Geography 1.** Characterize objective area, including country(s), geographic limits of objective area (geographic or universal transverse mercator coordinates), and plan or operation (number and name).

- **Geography 2.** Describe and state the significance of objective area.

- **Geography 3.** Describe geographic terrain features (general description, key natural and manmade features).

- **Geography 4.** Describe flora and fauna. Include information of tactical value, e.g., plants and animals that would impede or assist movement routes, rates, massing, dispersal, identification and acquisition of forces; the effects on weapon capabilities; and security considerations.

- **Geography/Approaches.** Avenues of approach into objective area (road, rail, waterway, air) with most likely approach of reinforcements; obstacles, choke points, terrain features; special conditions (seasonal variations); fording sites (depth, width, type bottom); trafficability (transit).

- **Geography/Hydrography 1.** Provide hydrographic data (coastal, waterways, lakes), to include tidal activity; currents; temperatures; special conditions (seasonal variations); and depths and underwater obstacles.

- **Geography/Hydrography 2.** Identify water sources (type, source, location, capacity).

- **Geography/Hydrography 3.** Provide detailed terrain and/or hydrographic data

on landing beaches within the objective area to include nearshore and/or offshore bathymetric data (currents, tides, wave height, depth, reef conditions, location of sandbars, beach gradients, frontage, composition, obstacles).

- **Geography/Geospatial Information and Services 1.** Provide terrain data (i.e., prominent geographical or manmade structures that could be used as navigational aids for aircraft, troops, cruise missiles or precision-guided munitions [PGM]; and characteristics of slope, soil analysis or surface material) to determine trafficability.

- **Geography/Geospatial Information and Services 2.** Provide terrain maps, charts, overlays, imagery or pictomaps in both printed and digital form.

- **Geography/Geospatial Information and Services 3.** Provide ocean charts for deploying naval forces.

- **Geography/Meteorology and Oceanography 1.** Describe METOC conditions to support air, ground, and naval operations, artillery, surface-to-surface missile, cruise missile, PGMs, reconnaissance, surveillance and communications operations.

- **Geography/Meteorology and Oceanography 2.** Provide historical METOC data (including unusual conditions such as sandstorms, blizzards).

- **Geopolitical/Allies and Coalition Partners.** Assess true capabilities and vulnerabilities of non-US multinational forces.

- **Geopolitical/Intentions.** Determine country's strategic intentions. Identify country's criteria for success.

- **Geopolitical/Reaction 1.** Determine the reaction of potentially hostile, allied, or neutral international, political, civilian, military, and paramilitary elements to insertion of US forces into the AOR and/or JOA before or after initiation of hostilities. Will a third party intervene?

- **Geopolitical/Reaction 2.** Identify neighboring countries that have taken any measures or may attempt to disrupt US airlift and/or sealift operations. Describe their capabilities, e.g., units, tactics. Determine which resources will be used.

- **Geopolitical/Reaction 3.** Identify countries en route to or in the AOR and/or JOA which will or may deny US overflight, landing rights, or docking privileges.

- **Geopolitical/Reaction 4.** Determine which potential hostile and/or target countries in the AOR and/or JOA have detected US preparations to conduct or support military operations in the AOR and/or JOA. Estimate their reaction.

- **Host-Nation Support.** Describe logistics infrastructure existent within the coalition area for use by US and/or coalition forces. Estimate level of host-nation support that US forces can expect.

- **Host-Nation Support/Logistics.** Identify suitable beaches and/or terrain available for joint logistics over-the-shore operations.

- **Host-Nation Support/Ports 1.** Describe sea ports (port infrastructure, operational considerations, fuel, cargo handling, transshipment, security).

- **Host-Nation Support/Ports 2.** Describe airports (type, status, activity), defenses (friendly and unfriendly), combat operations, facilities, infrastructure, support facilities.

- **Host-Nation Support/Transportation 1.** Describe transshipment or transportation capability from air and sea ports. Identify major obstacles, choke points, limitations, and alternative routes.

- **Host-Nation Support/Transportation 2.** Identify critical C4 and transportation nodes which, if destroyed, would have an adverse impact on USTRANSCOM's ability to deploy and sustain US combat forces.

- **Indications and Warning 1.** Provide I&W of potential hostile attacks such as movement of aircraft to dispersal bases; unusual out of garrison deployments; distribution of wartime stores and supplies; changes in readiness, alert, and mobilization postures.

- **Indications and Warning 2.** I&W indicators of preparation by the objective country or opposition forces for action within a 24-hour period for the following: attack, withdraw without engaging, reinforce, defend, delay, conduct special or NBC operations.

- **Infiltration.** Identify and describe potential landing zones and drop zones, navigation landmarks and characteristics; availability to US forces; limitations on operations; choke points between insertion points and objective; and adversary forces threat information at zone and along route.

- **Information Warfare/Offensive.** Identify and describe offensive IW capabilities.

- **Information Warfare/Defensive.** Identify and describe defensive IW capabilities.

- **Intelligence/Adversary Capability.** Identify, locate, and describe country intelligence and CI capabilities by type (SIGINT, HUMINT, IMINT), with particular emphasis on key facilities, surveillance measures, and night vision capabilities; include agency, means, effectiveness, biases.

- **Lines of Communications 1.** Describe railways, to include status, description of network (graph, overlay, chart), and factors limiting use. List bridges, tunnels, ferries, locomotives, rolling stock, signal and control systems, railway gauge, terminals.

- **Lines of Communications 2.** Describe roadways to include status, description of network (graph, overlay, chart), factors limiting use, and bypass routes. List bridges, tunnels, ferries, fords, highway maintenance, vehicle types.

- **Lines of Communications 3.** Describe waterways (graph, overlay, chart); beaches suitable for amphibious landing (beach length, configuration, usable length); interruptions and obstacles; type of coastline; backshore, foreshore, and nearshore description (width, gradient, composition).

- **Lines of Communications 4.** List primary and exploitable modes of transportation (trucks, buses, river craft — government, public and commercial).

- **Lines of Communications 5.** Describe petroleum, oil, and lubricants (POL) (sources, reserves, natural gas stream, production, refining, storage, pipelines, pump and compressor stations, controls, storage tank farms, shipping terminals, distribution), to include development company and/or nation, vulnerabilities and exploitability by United States for its forces.

- **Lines of Communications 6.** Describe power grid (generating and distribution

networks, facilities, loads, maintenance, transmission lines, sources of energy, controls, blackout history, government organizations associated, development company and/or nation) to include vulnerabilities and exploitability by US forces.

- **Lines of Communications/Airfields.** Describe airfields (graph, overlay, chart — type, location, capacity, POL, parking areas, aircraft, base operations and facilities, development company and/or nation) and factors limiting use and/or availability.

- **Lines of Communications/Information 1.** Describe public information media and telecommunications to include status, controlling authority, signal allocation; radio and television broadcasts; print and newspapers; communications network, technologies, equipment and operations.

- **Lines of Communications/Information 2.** Determine status of civil telecommunications systems; identify existing links. Are sufficiently trained personnel available to fully man and operate the systems? Identify specific skill shortages. Are facilities secured (by whom)?

- **Lines of Communications/Seaports.** Describe the threat country's seaports (port infrastructure, operational considerations, fuel, cargo handling, transshipment, security, development company and/or nation). Identify vulnerabilities, port operation, commercial and military shipping traffic.

- **Military Assistance 1.** Identify countries committed to providing military assistance (legal, de facto); military advisors, and other personnel already present (noncombatants, medical, engineers, by country, location, type of assistance); combatants or paramilitary (strengths, locations).

- **Military Assistance 2.** Identify foreign technologies (communications, computers, software) or contractor services, and construction (type of work, frequency, purpose, equipment, location, country or company); and foreign non-weapons military materiel (trucks, heavy equipment).

- **Military Assistance 3.** Identify foreign or US materiel and services required by the threat nation. Can the country operate systems, forces, industries without foreign personnel, equipment, or supplies? How long? What is the impact of cutoff of foreign support? Status of LOCs.

- **Military Capabilities/Air Defense 1.** Assess the capabilities and readiness, doctrine, tactics, vulnerabilities, intentions, location, disposition, and sustainability of air defense forces (surface-to-air missile [SAM], anti-aircraft artillery [AAA], radar, sensors) and their support facilities.

- **Military Capabilities/Air Defense 2.** Identify countries in AOR and/or JOA which show indications of preparing air defense forces to intercept US and/or allied air operations. Describe the long-range fighter intercept capabilities of the potential threat air defense forces (adversary and neighboring countries).

- **Military Capabilities/Air Defense 3.** Locate and identify capability to support ground forces with combat air and air defense resources (en route to and within the objective area), particularly at or around the forward edge of the battle area.

- **Military Capabilities/Air Defense 4.** Detect, locate, and identify SAM and AAA threat emitters and associated weapons along ingress and egress routes and within the objective area; determine operational status, readiness and duty cycle of air defense radars within objective area of influence.

- **Military Capabilities/Air Defense 5.** Detect SAM launch.

- **Military Capabilities/Air Defense, EW, and/or ground control intercept (GCI) Radars.** Determine precise location and status of EW and/or GCI radar sites.

- **Military Capabilities/Air Operations 1.** Assess the capabilities, readiness, sortie rates, munitions, doctrine, tactics, vulnerabilities, intentions, location, disposition (count, track, identify, classify) and sustainability of threat air forces.

- **Military Capabilities/Air Operations 2.** Detect, identify by type, and locate threat aircraft launch event in operational area and determine type of onboard munitions.

- **Military Capabilities/Air Operations 3.** Track inflight threat aircraft within the operational area.

- **Military Capabilities/Antimissile Defense/Adversary 1.** Detect and identify any antimissile defense systems, especially those that could affect cruise missiles along flight path. Determine operational status of each such system.

- **Military Capabilities/Antimissile Defense and/or Adversary 2.** Detect, identify by type, and locate antimissile launch event.

- **Military Capabilities/C4I 1.** Detect, locate, classify, characterize and identify command posts and/or bunkers by type unit, computers, communications architecture and critical C4I nodes.

- **Military Capabilities/C4I 2.** Describe country communications profile (type of information on circuit, type of communications, communications table of organization and equipment, pattern of employment, COMSEC equipment and methods, location), including computer connectivity.

- **Military Capabilities/C4I 3.** Detect wartime reserve mode usage and anticipated countermeasures.

- **Military Capabilities/C4I 4.** Determine adversary vulnerability to C2W; list communications of military significance including computers and susceptibility to C2W actions.

- **Military Capabilities/C4I 5.** Assess adversary C2W C2-attack and C2-protect capabilities and indications of employment.

- **Military Capabilities/Camouflage, Concealment, and Deception 1.** Detect, identify, locate and characterize adversary CCD techniques with emphasis on use of decoys.

- **Military Capabilities/Camouflage, Concealment, and Deception 2.** Determine the deception techniques the adversary will most likely accept as truth. Assess the adversary's ability to pierce US CCD plan.

- **Military Capabilities/Electronic Order of Battle.** Assess the adversary's electronic resources (including country

high value airborne resources, EW, GCI, fire control, tracking, and acquisition radars) capabilities. Evaluate resource location and disposition, sustainability and vulnerabilities.

- **Military Capabilities/EW.** Assess capability to perform EW, C2W, suppression of enemy air defenses, beaconing, interference, jamming and intrusion, and electronic protection to include location, platform, type, specifications, and parametrics of equipment.

- **Military Capabilities/Ground Order of Battle 1.** Determine strength, status, location and identification of adversary forces with particular emphasis on armor, mechanized infantry, artillery, air defense, infantry, theater missile, nuclear, biological and chemical warfare units and munitions.

- **Military Capabilities/Ground Order of Battle 2.** Identify, describe and locate front-line adversary troop movements.

- **Military Capabilities/Ground Order of Battle 3.** Detect, classify and locate possible assembly, staging, dispersal, repair and resupply areas with emphasis on mechanized and armored vehicles.

- **Military Capabilities/Ground Order of Battle 4.** Detect, locate, classify, identify and determine composition of hostile forces capable of reinforcing the area and identify likely reinforcement routes. Identify, locate and describe adversary follow-on forces and resupply capability.

- **Military Capabilities/Ground Order of Battle 5.** Detect, locate, and identify by type anti-armor and antipersonnel mines, ditches, barriers, antitank traps, obstacles, field defensive positions, and night vision capabilities along potential assault routes and within vicinity of objective area.

- **Military Capabilities/Logistics 1.** Locate and identify combat service and support units, to include: transportation units; forward logistics bases; repair and repair facilities; ammunition supply points and storage areas; and POL sites.

- **Military Capabilities/Logistics 2.** Identify military units which are experiencing equipment or logistics problems and identify the causes. Assess how these problems are affecting the unit mission.

- **Military Capabilities/Naval 1.** Identify, describe, detect and locate threat naval forces (including coast guard and maritime border guard) to include type, number, capability, equipment, weapons, readiness, doctrine, tactics, munitions, vulnerabilities, disposition and status.

- **Military Capabilities/Naval 2.** Identify all surface, subsurface or air contacts within 150 nautical miles of battle group.

- **Military Capabilities/Naval 3.** Detect, identify, classify, and track adversary surface warships.

- **Military Capabilities/Naval 4.** Detect, identify, classify, and track adversary submarines.

- **Military Capabilities/Naval 5.** Detect, classify, identify, locate, and track (time, position, course, speed) designated naval surface targets within adversary naval task force (include target description data, such as size, shape, and composition needed for weaponeering).

- **Military Capabilities/Naval 6.** Detect, locate, and characterize all other vessels

capable of defending the target within 50 nautical miles of the target vessel, or other objects that may inhibit missile acquisition of the target.

- **Military Capabilities/Naval 7.** Identify, locate and describe country shore-based defensive positions, to include fixed and mobile antiship cruise missile systems, beach defenses, coastal artillery, coastal defense units, and coastal surveillance networks.

- **Military Capabilities/Paramilitary.** Describe country's paramilitary and/or indigenous forces, internal security forces or police (tables of organization and equipment, strength, type, number, capability, equipment, weapons, night operations).

- **Military Capabilities/Rear Area Issues 1.** Determine presence, location, strength, status, and identification of conventional forces isolated in friendly rear areas. Focus on those forces no longer controlled by higher headquarters that could continue combat operations outside adversary's intent.

- **Military Capabilities/Rear Area Issues 2.** Detect, identify and locate anti-US subversive elements within coalition force nations.

- **Military Capabilities/Rear Area Issues 3.** Describe adversary or sympathizers ability to infiltrate US deployment bases to conduct sabotage or subversive operations or attacks.

- **Military Capabilities/Rear Area Issues 4.** Detect presence, identity, location, strength, and activity of drug forces in the operational area.

- **Military Capabilities/Rear Area Issues 5.** Describe coalition and/or host nation foreign intelligence and security services' abilities to effectively collect and willingness to provide threat information in support of force protection efforts.

- **Military Capabilities/Rear Area Issues 6.** Describe the intelligence collection threat to friendly forces from foreign intelligence and security forces.

- **Military Capabilities/SOF-Adversary 1.** Determine presence, location, strength, doctrine, tactics, status and identification of country special operations forces. Include paramilitary forces and elements which engage in sabotage, espionage, terrorism.

- **Military Capabilities/SOF-Adversary 2.** Determine country special operations and psychological operations (PSYOP) plans, programs, and capabilities.

- **Military Capabilities/Space 1.** Describe country's access to space-based intelligence systems or products. Identify types of products or systems and which country and/or consortium provides the access and/or products. Locate ground station downlinks.

- **Military Capabilities/Space 2.** Assess country's ability to deny US use of space systems.

- **Military Capabilities/Surface-to-Surface Missiles (SSM) 1.** Describe, detect, classify by type, identify, and discriminate SSM or theater ballistic missiles (TBM), particularly those with mobile launchers within range of the objective area.

- **Military Capabilities/SSM 2.** Detect, identify by type, and locate missile (SSM, TBM) launch event (friendly, threat, unknown): (a) locate, identify and track inflight theater missiles; (b) discriminate

warhead type; (c) project impact point; (d) impact time and/or place, effect.

- **Military Capabilities/SSM-Antiship.** Detect, identify, classify, and track country SSM and/or antiship missiles within range of the naval task force. Detect and identify antishipping launches within the AOR and/or JOA.

- **Military Capabilities/Training and Readiness 1.** Assess general training level of country military units. Assess general level of military equipment maintenance and/or repair.

- **Military Capabilities/Training and Readiness 2.** Describe the readiness posture of military forces, both hostile and friendly, in the AOR and/or JOA.

- **Military Capabilities/Weapons.** Describe weapon systems and major military equipment items (both indigenous and foreign). Include type, availability, performance characteristics, strengths, vulnerabilities, maintenance and logistic capabilities, suppliers, training.

- **Military/General.** Describe uniform and equipment markings of adversary, coalition, UN.

- **Military/Intentions or Strategy 1.** Assess adversary force leadership's intentions (attack, defend, withdraw, reinforce, or delay). Determine adversary commander's campaign plan. Describe adversary's military strategy.

- **Military/Intentions or Strategy 2.** Assess adversary radical employment of "last ditch" weapons or tactics.

- **Military/Occupation Policy.** Identify measures military forces have implemented in occupied areas for physical and operations security and to control the local population and resources. Identify incidents which have occurred between occupation forces and the local population.

- **Noncombatant Evacuation Operation.** Update noncombatant evacuation operation personnel information and adversary counter-tactics. Determine permissive or non-permissive environment.

- **Personnel/Allied.** Locate, identify and determine status of allied prisoners of war, hostages, and diplomats.

- **Personnel/EPW.** Estimate how many adversary troops will surrender. Describe their general medical condition, available food supplies, morale, and ability or will to resist EPW controls.

- **Personnel/Morale 1.** Determine the health of opposing forces. Describe degree of nutrition, affects of local diseases, extreme environmental conditions and flora and fauna which adversely affects their health. Determine the causes and impact of health issues upon their unit's mission and capabilities.

- **Personnel/Morale 2.** Determine morale of invading military forces; thoughts about the war; opinion of their military and political leadership; opinion of military capability and resolve of the US. Determine the impact of this morale upon unit mission and capabilities.

- **Personnel/Morale 2.** Identify military units which are experiencing discipline problems and determine the causes. Assess how this will impact their mission.

- **Personnel/Morale 3.** Identify social, cultural, ethnic, religious, or political friction or animosities which exist among adversary military personnel.

- **Personnel/Morale 4.** Determine what the civilian and military personnel of the host nation think of the United States and of the military forces in their country. Describe any incidents of internal subversion against US forces or personnel.

- **Personnel/Neutrals.** Locate, identify and determine status of US travelers, businessmen.

- **Psychological Operations.** Identify items of US or other friendly PSYOP to which the adversary forces have been exposed. Assess the reaction of military forces to those materials.

- **Public Affairs.** Determine releasability of operations information (unclassified) to the media.

- **Sea Mines and Obstacles 1.** Describe mine warfare capability.

- **Sea Mines and Obstacles 2.** Detect, locate, and classify by type and number, surface, subsurface, or land mines and obstacles within vicinity of naval task force or designated landing beaches.

- **Sea Mines and Obstacles 3.** Locate and track untethered live sea mines.

- **Special Operations Forces/US 1.** Provide support to prioritize SOF targets and selection of ingress and/or egress routes.

- **Special Operations Forces/US 2.** Determine possible effective PSYOP techniques.

- **Space.** Determine if threat nation is exploiting US satellite systems for any military-related system.

- **Strategic Lift.** Determine the status of LOCs connecting US and/or coalition forces with allies and/or supply nodes.

- **Targets 1.** Determine country strategic and operational centers of gravity.

- **Targets 2.** Identify, describe, prioritize and locate fixed and mobile targets. Include critical strategic, operational and tactical facilities, airfields, offensive and defensive weapons systems, C4I facilities, troop concentrations and other items of interest.

- **Targets 3.** Assess target vulnerabilities.

- **Targets 4.** Determine effect (possible political, economic, or sociological impact) of damage or destruction of the target on the populace or the country's warmaking potential.

- **Targets 5.** Provide comprehensive list and geographical position of all protected facilities such as hospitals, religious shrines, art treasures.

- **Targets 6.** Determine which specific transportation, media, industrial, communications, or other infrastructures need to be protected for intelligence purposes, for the restoration and/or restructuring phase, or for use by US and/or coalition forces.

- **Targets 7.** Provide target identification, including target name, mission number, Basic Encyclopedia number, target coordinates, category codes, safe area number, and country.

- **Targets 8.** Provide contingency targeting and associated planning materials, to include imagery, maps, charts, and target descriptions. Provide updates during conflict.

- **Targets 9.** Nominate target sets based upon violations of war termination agreements (postconflict).

- **Targets/Acquisition.** Identify unique characteristics in target appearance and objects in target vicinity that contribute to or inhibit accurate scene generation for target acquisition (include varying weather, lightning, and seasonal conditions).

- **Targets/Area Activity.** Describe area activity on target (daily, weekly, monthly, seasonal, operational routine), and in target vicinity (daily, weekly, monthly, seasonal, operational routine in civilian neighborhood, industrial complex, business).

- **Targets/Communications and Information Infrastructure.** Describe target communications and information infrastructure to include type (telephone, radio, satellite communications, data fax, computer to computer); information security methods and procedures; visual signals or noise; and facilities (switches, power, antenna arrays, cables, personnel).

- **Targets/Physical Description 1.** Describe target physical layout or functional organization key component list, critical damage or stress point.

- **Targets/Physical Description 2.** Describe target facility construction, type material, strength of walls, depth of walls, and effects of different types of munitions on facility.

- **Targets/Power Sources.** Describe target, primary and alternate power sources (number, type, location, conduits location and type); associated facilities (transformers, switches, yards, relays, spares); fuel supply (types above and below, or partially below, ground location).

- **Targets/Security.** Locate target security posts, bunkers, trenches, and describe target security procedures to include patrols, lighting, detection systems, barriers and obstacles, entry, internal procedures and personnel access.

- **Targets/Security Forces.** Describe adversary ground reaction capability to defend target, to include dedicated or incidental capabilities (strength, equipment, training, weapons, reaction time).

- **Terrorism/Narcotics.** Describe terrorist- or narcotics-related threats that jeopardize combatant command OPLANs. Include adversary or supporting groups and organizations; likely areas of operation or targets; tactics and methods; training areas; and hideouts.

- **Threat 1.** Determine threat to US personnel and advisors.

- **Threat 2.** Identify safe houses (disposition, size and location).

- **Weapons of Mass Destruction (WMD) 1.** Determine if the country possesses and if it will use WMD.

- **Weapons of Mass Destruction 2.** Identify and classify facilities used for production or storage of WMD. Locate, identify, and classify threats, precise

location of suspected weapon fabrication, assembly, and storage required.

- **Weapons of Mass Destruction 3.** Describe the posture and disposition of country NBC munitions, delivery systems, and units. Confirm or deny presence of, and locate and identify, NBC warfare-capable units. Characterize and determine types and quantities of NBC munitions possessed by the country.

- **Weapons of Mass Destruction 4.** Identify threat forces NBC protection, decontamination facilities, and capabilities (locations and types).

APPENDIX C
INTELLIGENCE DISCIPLINES

This appendix is a classified supplement provided under separate cover. The classified Appendix expands on information contained in Joint Pub 2-01, "Joint Intelligence Support to Military Operations." Annexes have been included for each of the intelligence collection disciplines: HUMINT, IMINT, SIGINT, MASINT, and OSINT.

ANNEX A Human Intelligence (HUMINT) (U)
ANNEX B Imagery Intelligence (IMINT) (U)
ANNEX C Signals Intelligence (SIGINT) (U)
ANNEX D Measurement and Signature Intelligence (MASINT) (U)
ANNEX E Open-Source Intelligence (OSINT) (U)

Intentionally Blank

APPENDIX D
INTELLIGENCE ESTIMATE

The intelligence estimate is an appraisal of available intelligence on a specific situation used to determine the courses of action open to the adversary and the probability of their adoption. The format for the intelligence estimate is included below.

SAMPLE INTELLIGENCE ESTIMATE FORMAT

INTELLIGENCE ESTIMATE

SECURITY CLASSIFICATION

Originating Section Issuing Headquarters*
Place of Issue
Day, Month, Year, Hour, Zone

INTELLIGENCE ESTIMATE NUMBER**

( ) REFERENCES: a. Maps and Charts.
b. Other relevant documents.

1. ( ) Mission. State the assigned task and its purpose. The mission of the command as a whole is taken from the commander's mission analysis, planning guidance, or other statement.

2. ( ) Adversary Situation. State conditions that exist and indication of effects of these conditions on adversary capabilities and the assigned mission. This paragraph describes the operational area, the adversary military situation, and the effect of these two factors on adversary capabilities.

a. ( ) Characteristics of the Operational Area. Discuss the effect of the physical characteristics of the operational area on military activities of both combatants. If an analysis of the area has been prepared separately, this paragraph in the intelligence estimate may simply refer to it, then discuss the effects of the existing situation on military operations in the area.

(1) ( ) Military Geography

(a) ( ) Topography

* When this estimate is distributed outside the issuing headquarters, the first line of the heading is the official designation of the issuing command, and the ending of the estimate is modified to include authentication by the authorizing section, division, or other official according to local policy.

** Normally, these are numbered sequentially during a calendar year.

SECURITY CLASSIFICATION

1. ( ) Existing Situation. Describe relief and drainage, vegetation, surface materials, cultural features and other characteristics in terms of their effect on key terrain, observation, fields of fire, obstacles, cover and concealment, avenues of approach, lines of communications, and landing areas and zones.

2. ( ) Effect on Adversary Capabilities. Discuss the effect of topography on broad adversary capabilities such as attack and defense, describing generally how the topography affects each type of activity. The effect on employment of nuclear, biological, and chemical (NBC) weapons; amphibious, airborne, or air-landed forces; surveillance devices and systems; communications equipment and systems; electronic warfare; psychological operations, operations security and military deception; logistic support; and other appropriate considerations should be included.

3. ( ) Effect on Friendly Course of Action (COA). Discuss the effects of topography on friendly forces' military operations (attack, defense) in the same fashion as for adversary capabilities in the preceding subparagraphs.

(b) ( ) Hydrography

1. ( ) Existing Situation. Describe the nature of the sea and the coastline within the amphibious objective area; adjacent islands; location, extent, and capacity of landing beaches and their approaches and exits; nature of the offshore approaches, including type of bottom and gradients; natural obstacles; surf, tide, and current conditions.

2. ( ) Effect on Adversary Capabilities. Discuss the effects of the existing situation on broad adversary capabilities.

3. ( ) Effect on Friendly COAs, Discuss the effects of the existing situation on broad COAs for friendly forces.

(c) ( ) Climate and Weather

1. ( ) Existing Situation. Describe temperature, cloud cover, visibility, precipitation, light data, and other climate and weather conditions and their general effects on roads, rivers, soil trafficability, and observation.

2. ( ) Effect on Adversary Capabilities. Discuss the effects of the existing climate and weather situation on broad adversary capabilities.

3. ( ) Effect on Friendly COAs. Discuss the effects of the existing climate and weather situation on broad COAs for friendly forces.

(2) ( ) Transportation

(a) ( ) Existing Situation. Describe roads, railways, inland waterways, airfields, and other physical characteristics of the transportation system; capabilities of the transportation system in terms of rolling stock, barge capacities, and terminal facilities; and other pertinent data.

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of the existing transportation system and capabilities on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Discuss the effects of the existing transportation system and capabilities on broad COAs for friendly forces.

(3) ( ) Telecommunications

(a) ( ) Existing Situation. Describe telecommunications facilities and capabilities in the area.

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of the existing telecommunications situation on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Discuss the effects of the existing telecommunications situation on broad COAs for friendly forces.

(4) ( ) Politics

(a) ( ) Existing Situation. Describe the organization and operation of civil government in the operational area.

(b) ( ) Effect on Adversary Capabilities. Consider the effects of the political situation on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Consider the effects of the political situation on broad COAs for friendly forces.

(5) ( ) Economics

(a) ( ) Existing Situation. Describe industry, public works and utilities, finance, banking, currency, commerce, agriculture, trades and professions, labor force, and other related factors.

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of the economic situation on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Consider the effects of the economic situation on broad COAs for friendly forces.

(6) ( ) Sociology

(a) ( ) Existing Situation. Describe language, religion, social institutions and attitudes, minority groups, population distribution, health and sanitation, and other related factors.

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of the sociological situation on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Discuss the effects of the sociological situation on COAs for friendly forces.

(7) ( ) Science and Technology

(a) ( ) Existing Situation. Describe the level of science and technology in the operational area.

(b) ( ) Effect on Adversary Capabilities. Discuss the effects of science and technology on broad adversary capabilities.

(c) ( ) Effect on Friendly COAs. Discuss the effects of science and technology on broad COAs for friendly forces.

b. ( ) Adversary Military Situation (Ground, Naval, Air, Other Service)

(1) ( ) Strength. State the number and size of adversary units committed and adversary reinforcements available for use in the operational area. Ground strength, air power, naval forces, NBC weapons, electronic warfare, unconventional warfare, surveillance potential, and all other strengths (which might be significant) are considered.

(2) ( ) Composition. Outline the structure of adversary forces (order of battle) and describe unusual organizational features, identity, armament, and weapon systems.

(3) ( ) Location and Disposition. Describe the geographic location of adversary forces in the area, including fire support elements; command and control facilities; air, naval, and missile forces; and bases.

(4) ( ) Availability of Reinforcements. Describe adversary reinforcement capabilities in terms of ground, air, naval, missile, and NBC forces and weapons, terrain, weather, road and rail nets, transportation, replacements, labor forces, prisoner of war policy, and possible aid from sympathetic or participating neighbors.

(5) ( ) Movements and Activities. Describe the latest known adversary activities in the area.

(6) ( ) Logistics. Describe levels of supply, resupply ability, and capacity of beaches, ports, roads, railways, airfields, and other facilities to support supply and resupply. Consider hospitalization and evacuation, military construction, labor resources, and maintenance of combat equipment.

(7) ( ) Operational Capability to Launch Missiles. Describe the total missile capability that can be brought to bear on forces operating in the area, including characteristics of missile systems, location and capacity of launch or delivery units, initial and sustained launch rates, size and location of stockpiles, and other pertinent factors.

(8) ( ) Serviceability and Operational Rates of Aircraft. Describe the total aircraft inventory by type, performance characteristics of operational aircraft, initial and sustained sortie rates of aircraft by type, and other pertinent factors.

(9) ( ) Operational Capabilities of Combatant Vessels. Describe the number, type, and operational characteristics of ships, boats, and craft in the naval inventory; base location; and capacity for support.

(10) ( ) Technical Characteristics of Equipment. Describe the technical characteristics of major items of equipment in the adversary inventory not already considered (such as missiles, aircraft, and naval vessels).

(11) ( ) Electronics Intelligence. Describe the adversary intelligence-gathering capability using electronic devices.

(12) ( ) Information Warfare. Describe the adversary offensive and defensive IW capabilities.

(13) ( ) NBC Weapons. Describe the types and characteristics of NBC weapons in the adversary inventory, stockpile data, delivery capabilities, NBC employment policies and techniques, and other pertinent factors.

(14) ( ) Significant Strengths and Weaknesses. Discuss the significant adversary strengths and weaknesses perceived from the facts presented in the preceding subparagraphs.

SECURITY CLASSIFICATION

c. ( ) Adversary Unconventional and Psychological Warfare Situation

(1) ( ) Guerrilla. Describe the adversary capability for, policy with regard to, and current status in the area of guerrilla or insurgent operations.

(2) ( ) Psychological. Describe adversary doctrine, techniques, methods, organization for, and conduct of psychological operations in the operational area.

(3) ( ) Subversion. Describe adversary doctrine, techniques, methods, organization for, and conduct of subversion in the operational area.

(4) ( ) Sabotage. Outline adversary organization and potential for and conduct of sabotage in the operational area.

3. ( ) Adversary Capabilities

a. ( ) Listing each adversary capability that can affect the accomplishment of the assigned mission. Each adversary capability should contain information on the following:

(1) ( ) What the adversary can do.

(2) ( ) Where they can do it.

(3) ( ) When they can start it and get it done.

(4) ( ) What strength they can devote to the task.

b. ( ) In describing adversary capabilities, the J-2 must be able to tell the commander what the adversary can do using its forces in a joint environment. First, of course, the J-2 must assess the adversary's ground, naval, and air forces. It is customary to enumerate separately the NBC and unconventional warfare capacities. Hypothetical examples follow.

(1) ( ) Ground Capabilities

(a) ( ) The adversary can attack at any time along our front with an estimated 6 infantry divisions and 2 tank divisions supported by 24 battalions of artillery.

(b) ( ) The adversary can defend now in its present position with 7 infantry divisions supported by 2 tank divisions and 16 battalions of medium and light artillery.

(c) ( ) The adversary can reinforce its attack (or defense) with all or part of the following units in the times and places indicated:

SECURITY CLASSIFICATION

UNIT	PLACE	TIME
315th Airborne Div	Vic RESOGA	8 hrs after starting time
41st Motorized	Vic CARDINAL	6 hrs after starting time

(2) ( ) Air Capabilities

(a) ( ) Starting now, and based on an estimated strength of 300 fighters and 100 medium bomber aircraft, the adversary can attack in the operational area with 240 fighter sorties per day for the first 2 days, followed by a sustained rate of 150 sorties per day, and 60 bomber sorties per day, for 1 day followed by a sustained rate of 48 sorties per day.

(b) ( ) Using airfields in the vicinity of _____, the adversary has sufficient transport sorties to lift one regiment in a single lift to airfields in the vicinity of ____ and ____ within 4 hours' flying time.

(3) ( ) Naval Capabilities. Starting now, the adversary can conduct sustained sea and air operations in the entire area with 6 DDs, 4 FFs, 1 CV, 7 SSNS, a mine force of 20 craft, and 70 gunboats and smaller craft now on station in the area.

(4) ( ) Nuclear Capabilities. The adversary can employ at any time and in any part of the operational area an estimated 40 to 60 nuclear weapons of yields from 2 to 50 kt delivered by cannon and rocket artillery, guided missile, and aircraft.

(5) ( ) Biological and Chemical Capabilities. The adversary can employ the biological and chemical agents ____, ____, and _____ in the operational area at any time delivered by air, cannon, and rocket artillery and by guided missile.

(6) ( ) Unconventional Warfare (UW) Capability. The adversary can conduct UW operations in the area within 10 days after starting the operation using dissident ethnic elements and the political adversaries of the current government.

(7) ( ) Joint Capabilities. The adversary can continue to defend its present position with 6 infantry divisions, supported by 16 artillery battalions and reinforced by 3 mechanized divisions within 8 hours after starting movement. Adversary defense also can be supported by 150 fighter sorties daily for a sustained period and by continuous naval surface and air operations employing 6 DDs, 4 FFs, 7 SSNS, and 1 CV.

4. ( ) Analysis of Adversary Capabilities. Analyze each capability in light of the assigned mission (considering all applicable factors from paragraph 2 above) and attempt to determine and give reasons for the relative order of probability of adoption by the adversary. Discuss adversary vulnerabilities. In this paragraph, examine the adversary capability by discussing the factors that favor or militate against its adoption by the adversary. When applicable, the analysis of each capability should also include a discussion of adversary vulnerabilities attendant to that capability; i.e., conditions or circumstances of the adversary situation that render the adversary especially liable to damage, deception, or defeat. Finally, that analysis should include a discussion of any indications that point to possible adoption of the capability, as in the following:

a. ( ) Attack now with forces along the forward edge of the battle area ....

(1) ( ) The following factors favor the adversary's adoption of this capability:

(a) ( ) ....

(b) ( ) ....

(2) ( ) The following factors militate against the adversary's adoption of this capability:

(a) ( ) Road and rail nets will not support large-scale troop and supply movements necessary for an attack in the area.

(b) ( ) Terrain in the area does not favor an attack.

(3) ( ) Adoption of this capability will expose the adversary's west flank to counterattack.

(4) ( ) Except for minor patrol activity in the ___ area, there are no indications of adoption of this capability.

b. ( ) Delay from present positions along the _____ River line ....

(1) ( ) The following factors favor the adversary's adoption of this capability:

(a) ( ) There are several excellent natural barriers between the _____ River and the _____ Mountains.

(b) ( ) The effectiveness of the water barriers will improve, and trafficability on the upland slopes of the terrain barriers will deteriorate with advent of the monsoon.

(2) ( ) The following factors militate against the adversary's adoption of this capability:

(a) ( ) ....

(b) ( ) ....

(3) ( ) In the adoption of this capability, the adversary's lines of communications will be restricted by a limited road and rail net that can easily be interdicted.

(4) ( ) The following facts indicate adoption of this capability:

(a) ( ) Aerial photography indicates some preparation of barriers in successive positions.

(b) ( ) Considerable troop movement and prepositioning of floating bridge equipment along the water barriers have been detected.

5. ( ) Conclusions. Conclusions resulting from discussion in paragraph 4 above. Include, when possible, a concise statement of the effects of each capability on the accomplishment of the assigned mission. Cite adversary vulnerabilities where applicable. This paragraph contains a summary of adversary capabilities most likely to be adopted, listed in the order of relative probability if sufficient information is available to permit such an estimate. If appropriate, it should also include a concise statement of the effects of each adversary capability on the accomplishment of the assigned mission. Exploitable vulnerabilities should also be listed, where applicable.

a. ( ) Adversary Capabilities in Relative Probability of Adoption

(1) ( ) Defend in present locations with ....

(2) ( ) Delay from present positions along ....

(3) ( ) Reinforce the defense or delay with ....

(4) ( ) Conduct UW operations in the area ....

b. ( ) Vulnerabilities

(1) ( ) Adversary left (west) flank is open to envelopment by amphibious assault ....

(2) ( ) The adversary's air search radar coverage is poor in the left (west) portion of its defensive sector ....

SECURITY CLASSIFICATION

(Signed) _____

J-2

(The staff division chief signs the staff estimates produced by that division. If the estimate is to be distributed outside the headquarters, the heading and signature block must be changed to reflect that fact.)

ANNEXES: (By letter and title) Annexes should be included where the information is in graphs or of such detail and volume that inclusion makes the body of the estimate cumbersome. They should be lettered sequentially as they occur throughout the estimate.

DISTRIBUTION: (According to procedures and policies of the issuing headquarters)

Intentionally Blank

APPENDIX E
SECURITY

1. Overview

a. Security doctrine and procedures safeguard and protect lives, information sources, and operations, and facilitate the timely movement and/or flow and dissemination of raw data and finished intelligence. All phases of the intelligence cycle are dependent upon the proper implementation and enforcement of security procedures to prevent violations and compromises, and to provide valuable time-sensitive intelligence to commanders. In a crisis situation, especially in a multinational environment, the J-2 must continue to maintain and enforce thorough and effective security procedures.

b. The J-2 makes a major contribution to the success of operational missions through peacetime security planning and preparation of tailored support to potential operations as well as careful consideration of possible security-related contingencies. This preplanning is especially significant during MOOTW involving multinational forces, which complicates dissemination and releasability procedures. In all environments, the J-2 must consider and assess such issues as:

- Properly classifying and/or sanitizing intelligence material to ensure the timely flow of critical intelligence to the requester, while considering the security implications of intelligence exchanges; and
- Using effective CI to enhance deception planning and operations.

2. Personnel Security

a. Among intelligence professionals, vigilance is the watchword, and periodic security training for all personnel is the method used to stress awareness and rectify procedural deficiencies and shortcomings. Personnel security standards have been met if there is no reasonable basis for doubting the person's loyalty to the US Government. Unified commanders and/or their designees are authorized to grant, deny, or revoke personnel security clearances (Top Secret, Secret, Confidential, and Limited Access Authorization) for personnel who have never been determined to be eligible for a clearance; revocation or denial of a clearance can only be done by the component that originally granted the clearance. Unified commanders can grant interim clearances, administratively withdraw clearances, and grant or deny access to classified information per the guidelines contained in DOD 5200.2-R, "DOD Personnel Security Program." The Services' senior officials of the intelligence community (SOICs) or their designees may grant SCI access for their respective Military Departments. The Director, DIA is responsible for OSD, Joint Staff, the Defense Agencies, and DOD Field Activities (less NSA/CSS and NRO).

b. An interlocking and mutually supporting series of program elements (e.g., need to know, investigation, binding contractual obligations on those granted access, security education and awareness, and individual responsibility) provides reasonable assurances against compromise of classified information. The primary security principle in safeguarding classified information is to ensure that it is accessible only by those persons with an appropriate clearance, access approval, clearly identified need to know, and an appropriate indoctrination (for SCI).

3. Sensitive Compartmented Information Facility

Before SCI can be handled, processed, or stored, a SCIF must be accredited based on established physical security guidelines. The SSO is the POC for information on accreditation authorities and SCIF physical security guidelines.

a. **Establishing and Accrediting a SCIF**

- Temporary and/or Emergency SCIFs

  •• A SCIF at any level of accreditation may be established upon the verbal order of a general and/or commander during declared hostilities or general war. Reconciliation of SCIF activation and operational data will be made no more than 180 days after SCIF activation.

  •• For operational contingencies, and with prior DIA coordination, a SOIC may approve a temporary SCIF for up to 60 days. DIA will assign a SCIF identification number and retain authority to cancel, extend, or change the accreditation. There are no specific physical requirements for such a SCIF, although sound attenuation problems should be addressed, the SCIF should be staffed around-the-clock, and appropriate guards should monitor and/or patrol the area.

  •• A tactical SCIF is a military field operation established during crisis, contingency, or exercise. A tactical SCIF can be set up and temporarily accredited by a SOIC. This authority may be further delegated in writing to one lower level of command. The local approving authority may require use of a local tactical deployment checklist. The element authorizing establishment of a tactical SCIF notifies the accreditation authority and DIA by message before starting SCIF operations. The message format is shown in Figure E-1.

  •• A tactical SCIF may be operated within a randomly selected structure for the duration of an exercise. If reused within 36 months for SCI discussion, a technical surveillance countermeasures evaluation is recommended. During crisis and hostilities, there is no restriction over SCI discussion within a tactical SCIF.

  •• A temporary secure working area (TSWA) is a temporarily accredited facility used no more than 40 hours per month for handling, discussing, or processing SCI. SOICs and unified command senior intelligence officers (SIOs) may approve TSWAs for all levels of SCI. SOICs, SIOs and DIA may approve electronic processing of SCI in a TSWA. Approval of temporary storage of SCI, not to exceed 6 months, may be granted by DIA or a Service.

  •• Shipboard SCIFs. A shipboard tactical facility requires submission of the shipboard accreditation checklist to the Navy accreditation authority. Temporary shipboard accreditation is approved by SOIC Navy for units which may deploy for emergency contingencies, not to exceed a 12-month deployment period. Permanent accreditation is approved by SOIC DIA.

  •• Aircraft SCIFs. Aircraft will be accredited through established accreditation channels. Transports and courier aircraft transporting SCI material between airfields do not require accreditation; however, compliance with SCI material and communications directives are mandatory. Aircraft temporarily configured for SCI missions by installing pallets, vans, or containers aboard, will be accredited by the

SAMPLE TACTICAL SENSITIVE COMPARTMENTED INFORMATION FACILITY OPERATIONS MESSAGE FORMAT

FROM: (Originator's Message Address)

TO: SSO DIA//DAC-2A//

CLASSIFICATION

SUBJECT: TACTICAL SCIF OPERATION (U)

1. (U) DIA SCIF-ID number of parent SCIF.
2. (U) Name of Tactical SCIF.
3. (U) Deployed from location.
4. (U) Deployed to location.
5. (U) SCI level of operations.
6. (U) Operational period.
7. (U) Name of exercise or operation.
8. (U) Identification of facility used for SCIF operations (e.g., vans, buildings, tents).
9. (U) Points of contact.
10. (U) Description of security measures.
11. (U) Comments.
12. (U) POC FOR THE ACTION: (name, office symbol, and telephone number).

Figure E-1. Sample Tactical Sensitive Compartmented Information Facility Operations Message Format

appropriate SOIC having SCI cognizance. Contingency and emergency deployment aircraft, operating with SCI processing aboard, may be operated as a tactical SCIF in accordance with Director, Central Intelligence Directive (DCID) 1/21, "Physical Security Standards for SCIFs."

b. **Tactical SCIF Security.** Although security is necessary for the integrity of a SCIF, the SSO determines the degree of security to be maintained, taking the operators' needs and the local situation into account. Security should support, rather than restrict, the mission. Recommended guidelines for maintaining SCIF security include the following.

- Staff the tactical SCIF with sufficient personnel as determined by the on-site security authority based on the local threat conditions.
- Locate the tactical SCIF within the supported headquarters' defense perimeter.
- Post armed guards to protect the entire perimeter of the SCIF compound. Maintain radio or wire communications with the guard and reserve force.
- Use a single entrance and access control procedures.

- Keep emergency destruction and evacuation plans current and displayed.
- Store SCI materials in lockable containers when not in use.
- Incorporate the SCIF physical security plan into the perimeter defense plan.
- Store no more intelligence than can be destroyed in a reasonable amount of time.

c. **Assignments of Foreign Representatives to a SCIF.** Prior to the assignment of foreign personnel to a SCIF, the subordinate joint force J-2 must consider the scope of the foreigner's role in relation to the environment. Foreign representatives in a SCIF should be physically located so that they may work effectively without being inadvertently exposed to restricted data. If a tactical SCIF is in a multinational environment with a US-only area, the US-only area must be kept separate from any multinational operations. The guard(s) must be a US citizen. The J-2, in coordination with the SSO, should ensure constant oversight of non-intelligence elements residing in the SCIF to ensure that there will be no compromise of operational matters.

4. Sanitizing and/or Releasing Intelligence

a. US government policy is to treat classified military information as a national security asset, which may be shared with foreign governments and international organizations only when there is a clearly defined advantage to the United States. US national interests require that foreign governments provide US classified information with a degree of security protection comparable to what it would receive while under US control. There are a number of international and bilateral security agreements in effect to ensure this. However, in exceptional cases it will be in US interests to make information available to a foreign government before concluding an agreement, even if the recipient government's safeguards appear inadequate. In these cases, when authorized by the National Disclosure Policy Committee (NDPC) as exceptions to policy, a balance is sought between US national interests and the security of the classified information.

b. National Disclosure Policy (NDP)-1 governs how the United States releases military information to foreign governments and international organizations and establishes eligibility criteria to receive releasable information. Detailed procedures for handling, processing, downgrading, release and sanitization of these materials exist. Key national security policy and security manuals are included in Appendix J, "References."

c. Intelligence information, even though it bears no restrictive control markings, may only be released in its original form to foreign governments or international organizations with the permission of the originator and in accordance with DCID 5/6, "Intelligence Disclosure Policy" and NDP-1. Information contained in intelligence products or reports of another intelligence community component, which bears no restrictive control markings, may be used by recipient intelligence community components in reports provided to foreign governments provided that the following is true.

- Foreign release occurs through established foreign disclosure and procedures.
- No reference is made to the originating agency or to the source documents upon which the released product is based.
- The information is extracted or paraphrased to ensure that the source or manner of acquisition of the intelligence

and/or location where the intelligence was collected (if relevant to protect sources or methods) is not revealed and cannot be deduced in any manner.

- RESTRICTED DATA and FORMERLY RESTRICTED DATA are prohibited from foreign dissemination under the provisions of Public Law 585, Atomic Energy Act of 1954, as amended.

d. Even though it bears no restrictive control markings, intelligence will not be released, either in its original form or otherwise, to foreign nationals or immigrant aliens (including those employed by, used by, or integrated into the US government) without the permission of the originator and in accordance with DCID 5/6, "Intelligence Disclosure Policy" and NDP-1.

e. An SSO can provide more detailed information on SCI policy and procedures, and the DISO assigned to the cognizant combatant command can help to seek exemptions to security policy from national agencies. The combatant commander is responsible for the release of intelligence and should request that intelligence producers tailor their product so as to minimize the use of caveats.

f. As shown in Figure E-2, and apart from the exceptions listed in Figure E-3, military information is divided into eight functional categories by the NDPC. In almost all cases, intelligence under consideration for release at the subordinate joint force J-2 level will be in Category 8. Combatant command requests for disclosure of NDPC-exception categories of intelligence information will be made in accordance with the policies and directives of the DOD, intelligence community members, or other office responsible for the information.

g. Classified information may only be disclosed when the following applies.

- Disclosure is consistent with US foreign policy and national security objectives concerning the recipient foreign government or international organization.

- Disclosure can be expected to result in a clearly identifiable advantage to the United States.

- It can be reasonably assumed that the disclosed information would not be used against US interests.

h. **Release Policies and Procedures.** J-2s should consider the following when determining whether to release classified information.

- Determine recipient country's eligibility to receive military intelligence. If the country is not eligible yet meets the conditions listed below, a request for exemption to NDP can be made through the combatant command's Foreign Disclosure Officer.

- Determine recipient's need to know. Any recipient, whether a member of the US military or a foreign government, must have a "need to know" before being provided with US intelligence. While determining need may be difficult, the J-2 may rely on common sense and knowledge of the situation. For example, Country X has a legitimate need to know about Country Y-sponsored terrorist activities in the region. However, since Country X faces no direct military threat from Country Y, it has no need to know and is not eligible to receive information on Country Y's order of battle. Where necessary, a decision may be based on political and/or military expediency.

- The gain must clearly outweigh the risk of compromising the source. This is most easily ensured by sanitizing the original

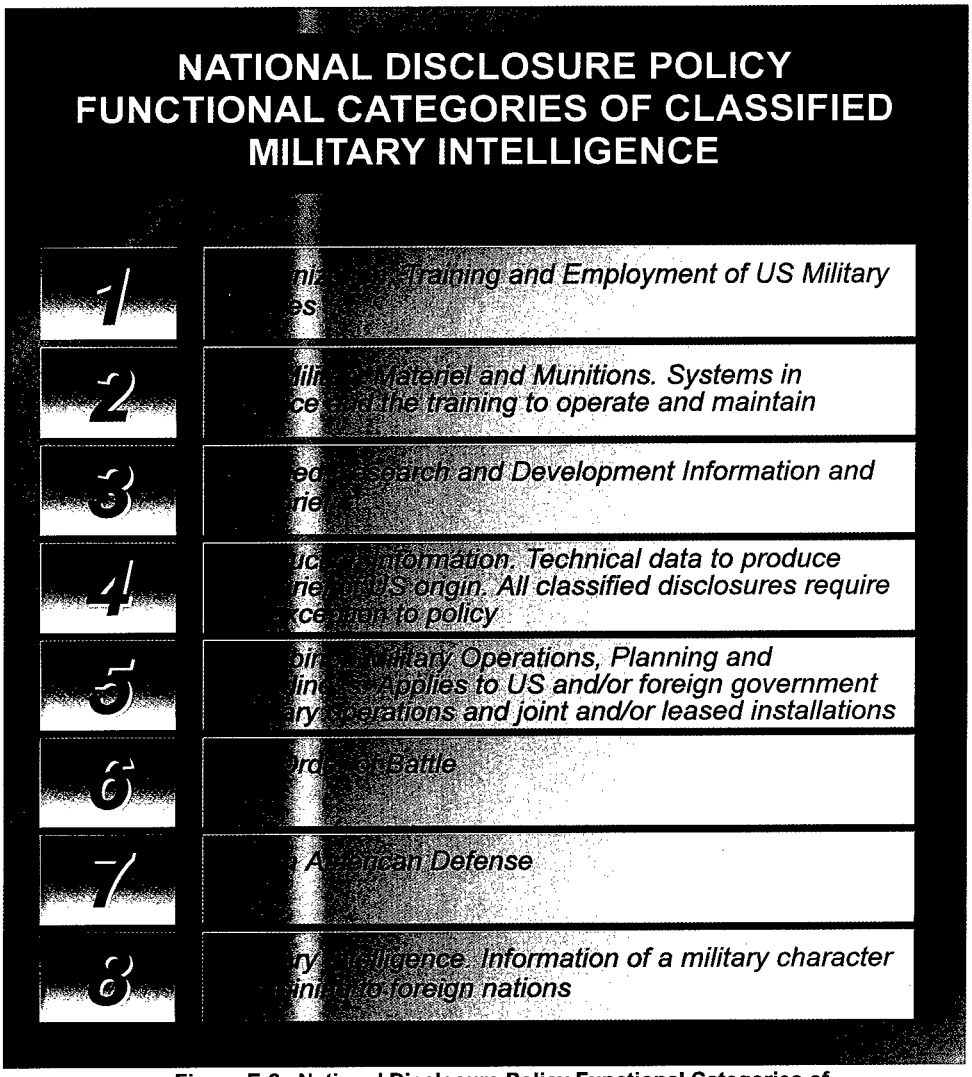


Figure E-2. National Disclosure Policy Functional Categories of Classified Military Intelligence

report to protect the source.

- Release intelligence only to the level of command necessary, as determined by the J-2.

- As noted above, except in exceptional circumstances, the organization receiving the intelligence must reasonably be expected to afford the same degree of protection against compromise as would US channels.

i. Key points on release of classified material are listed in Figure E-4.

5. ADP Security

a. The authority to permit the automated processing of intelligence information is vested in the Director, DIA, who has the responsibility to ensure that the risks posed during processing are outweighed by the gain. Specifically, this means that adequate security of contractor and DOD (less NSA/CSS) automated information systems and the

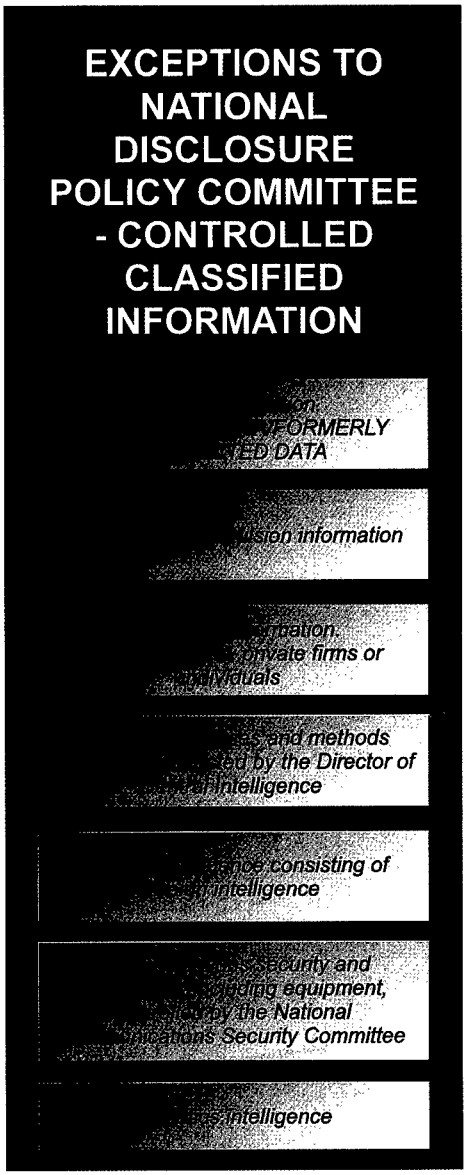


Figure E-3. Exceptions to National Disclosure Policy Committee-Controlled Classified Information

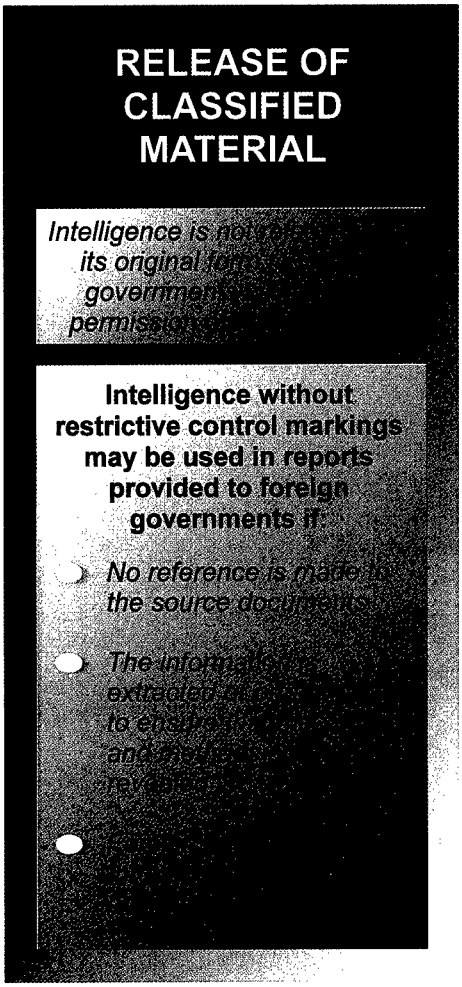


Figure E-4. Release of Classified Material

security of systems (networks) that store, process and/or transmit sensitive foreign intelligence information, are under the cognizance of the Director, DIA. DIA manages the DODIIS Computer Security Program in accordance with the appropriate DOD and DCI directives.

b. As far in advance of joint operations as possible, personnel responsible for establishing security (in coordination with those responsible for determining the information system and/or connectivity requirements) should contact DIA. They must inform DIA of the names and accreditation status of systems to be used during the operation, as well as planned inter-connectivity. DIA will work with planners to balance security requirements with operational requirements.

Intentionally Blank

APPENDIX F
DEPARTMENT OF DEFENSE SHARED PRODUCTION PROGRAM

1. Introduction

The DODIPP was established in response to Congressional mandate to reduce duplication of effort within the DODIPC. Central to the DODIPP concept is the sharing of production. Production responsibilities are assigned to capitalize on the analytical and production resources of the entire DODIPC to focus expertise and maximize output for the consumer. The structure is an explicit, logical division of activities, responsibilities, and accountability among national, Service, and combatant command production centers based on traditional roles as specified in title 10 of the United States Code and the national-level military intelligence requirements forums. The SPP is based on data bases produced by two or more intelligence production centers. These producers are responsible for all production based on the substantive topics in the shared data base.

2. Responsibilities

a. In the event of a crisis or war, defense production support will focus on the NMJIC, which will form intelligence work groups or intelligence task forces as necessary in accordance with designated responsibilities and procedures. RFIs/PRs from the crisis and/or engaged joint force will be transmitted to its combatant command VO which, if unable to satisfy the RFI/PR, will forward it to the NMJIC. All other RFIs/PRs relating to the crisis will be forwarded through normal VO chains of command to the NMJIC, which will be the single DOD VO for all other RFIs/PRs related to the crisis.

b. The Defense Intelligence Production Functional Manager (DI/DIA) is responsible for ensuring that DODIPC production supports the NMJIC during a crisis or conflict. The NMJIC will have the authority to assign PRs and reprioritize ongoing crisis-related production in coordination with the combatant commands. The Defense Intelligence Production Functional Manager will retain oversight of non-crisis-related DODIPC production, adjusting production schedules as necessary.

c. The Director, DI acts as the executive agent for production issues for the Director, DIA. Key responsibilities (for a complete list of responsibilities, see DOD-0000-151-YR, "DOD Intelligence Production Program") include the following:

- Evaluate DODIPP production center production and capabilities in conjunction with the combatant commands, Services, and appropriate Defense agencies through production program reviews at each DODIPC production center.

- Assign and change DODIPP responsibilities as required in coordination with the appropriate combatant command, Service, and Defense agency representatives.

- Assist production centers in developing needed capabilities; identify, coordinate, and program resource requirements to meet DODIPP responsibilities; and serve as an advocate for SPP resource planning and application.

- Initiate management coordination when problems arise, and mediate disagreements.

- Manage the coordination of SPP data base requirements and specifications to establish DOD-wide standards for applicable data elements, documentation, and communications. Provide implementation guidance and schedules for approved changes and monitor implementation.

- Maintain active, continuous, and meaningful communication with production centers on improving the production of substantive intelligence.

- Act as advocate for collection requirements to support the currency and validity of SPP production.

d. Based on DODIPP guidelines, Military Service intelligence chiefs are charged with the same responsibilities as the combatant commands for DODIPP tasks through Service channels (for a complete list of responsibilities see DOD-0000-151-YR, "DOD Intelligence Production Program") to include the following:

- Validating requirements and producing intelligence to satisfy title 10 responsibilities in support of the Service Secretaries' responsibilities.

- Coordinating and accomplishing planning, programming, and budgetary actions to support the SPP, including analytical, automated intelligence system and telecommunication capability requirements identified by production centers and supported commands.

- Ensuring that adequate training capabilities are available for current and future analytical intelligence personnel to support production responsibilities.

APPENDIX G
JOINT EXPLOITATION CENTERS

1. Overview

a. The exploitation of captured adversary equipment and documents and the interrogation and debriefing of EPW, detainees, refugees, and other captured adversaries, provides significant collection opportunities. The information obtained through this exploitation, coupled with that derived from other collection assets or resources, may provide the JFC (through the J-2) a more complete picture of an unfolding operation and adversary capability. The in-theater exploitation of these sources is accomplished at the three exploitation centers: the JCMEC, the JDEC, and the JIDC. (Figure G-1) Whenever possible, the three centers should be collocated in the same operational area to facilitate rapid exchange of data. Short-term exploitation of captured materiel and documents as well as interrogation or debriefing of EPWs, refugees and other sources may be of immediate tactical value. Such debriefings can provide information important for decisions regarding the targeting cycle and tempo of operations. Tactical exploitation by trained intelligence personnel must be accomplished as soon as possible and at the lowest possible tactical level. Long-term exploitation of the same material and sources at joint force level may provide valuable operational, strategic and technical data. Further exploitation may be continued out of theater where there are better facilities for detailed research and analysis. The JCMEC, JDEC, and JIDC all conduct exploitation in the AOR and/or JOA, but their functions are not limited solely to combat operations. Both peacekeeping operations and refugee relief, for example, could require confiscating weapons and contraband; and refugee relief could also require screening refugees for critical information. In MOOTW the names of these centers may be changed to reflect the type of operations being supported.

b. **Joint Captured Materiel Exploitation Center.** The recovery of adversary equipment is both a combatant command and national requirement. Subsequent exploitation of captured enemy equipment (CEE) can provide critical information on adversary strengths and weaknesses that may favorably influence operation planning. This exploitation is generally done in a JCMEC. Combatant commands or subordinate joint forces should notify the NMJIC through command channels that they require JCMEC support. This will ensure that appropriate Service component resources will be allocated.

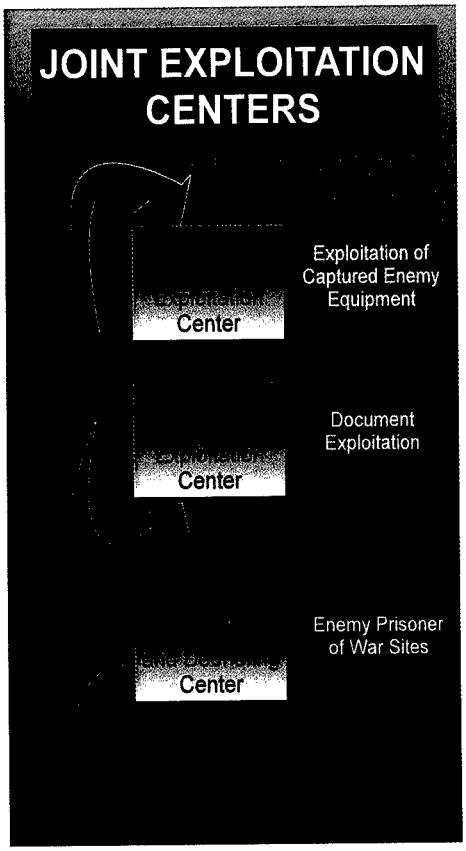


Figure G-1. Joint Exploitation Centers

- **Organization.** The Foreign Materiel Program is the focus for forming a JCMEC to conduct exploitation of CEE. A JCMEC is formed of Foreign Materiel Program personnel from the Services' technical intelligence organizations and Naval Explosive Ordnance Disposal. It is activated during periods of joint force deployments, deployed to the combatant command, and normally assigned to and under the combatant command (command authority) of the CINC. DIA supplies a Technical Intelligence Branch from which the J-2 exercises staff responsibility over all matters pertaining to CEE, including prioritizing requirements for CEE, technical intelligence reporting, and coordinating with the J-3 and J-4. The J-2 also evaluates the mission and situation and determines the potential for capturing adversary materiel. These factors determine the size and composition of the JCMEC.

- **Responsibilities.** The combatant command approves establishment of theater collection points recommended by the J-2 and sets the priority for the recovery and movement of CEE to those collection points and CONUS. The subordinate joint force and subordinate commands provide access to CEE collection points to JCMEC personnel and other supporting specialists. These personnel then evacuate CEE deemed to be valuable for intelligence or other DOD requirements. The exploitation of CEE below Army division and separate brigade, Marine Corps expeditionary force command element, and Navy and Air Force component levels is limited. Units below these levels are responsible for recovering adversary materiel and reporting its capture. Medical equipment and materiel should be exploited in the same manner as other CEE, except that cooperation and collaboration with local medical units should be established using Geneva Convention guidelines. Normally, a Service component commander or the joint force land component commander (if designated) establishes the JCMEC facility and provides or coordinates all necessary logistics, communications, siting, and transportation support for the JCMEC.

c. **Joint Document Exploitation Center.** Document exploitation, like equipment exploitation, is both a combatant command and national requirement. Generally, documents may be moved much more easily than CEE and will contain information on a large range of topics. Captured documents provide information on adversary intentions and planning (including deception); locations; dispositions; tactics; communications; logistics; morale; intelligence requirements and assessments; psychological operations efforts aimed at friendly forces, adversary forces, and the civil populace; and equipment use, status, and operation. The JDEC should be centralized, staffed, and equipped to be able to dispatch JDEC teams to lucrative targets (e.g., adversary field staff or command locations, facilities, or vehicles, airfields, or other facilities) as soon after capture as possible, or with maneuver units when such targets are anticipated. Combatant commands or subordinate joint forces requiring a JDEC should notify the NMJIC through command channels, requesting JDEC operations support.

- **Organization.** The DIA focus for forming a JDEC is the Document Exploitation Branch of the Directorate for Information Systems and Services. As with the JCMEC, it is activated during periods of joint force deployments, deployed to the combatant command, and normally assigned to and under the combatant command (command authority) of the CINC. The subordinate

joint force J-2 exercises staff responsibility over all matters pertaining to document exploitation, including prioritizing requirements, intelligence reporting, and coordinating with the subordinate joint force J-3 and J-4. The J-2 also evaluates the mission and situation and determines the potential for capturing adversary documents. These factors determine the size and composition of the JDEC.

- **Responsibilities.** The combatant command approves priority for the recovery and movement of documents to theater collection points and the CONUS as recommended by the J-2. The subordinate joint force and subordinate commands provide access to captured documents to JDEC personnel and other supporting specialists. These personnel evacuate documents deemed to be valuable for intelligence or other DOD requirements. Document exploitation capabilities exist at the Army corps, Army light infantry division, and in the command element of the Marine air-ground task force, with the organic capabilities of the Navy and Air Force being more limited. Units below these levels are responsible for recovering adversary documents and reporting their capture. Normally, a Service component commander or the joint force land component commander, if designated, establishes the JDEC facility and provides or coordinates all necessary JDEC personnel, logistics, communications, siting, and transportation support.

d. **Joint Interrogation and Debriefing Center.** The JFC normally tasks the Army component commander to establish, secure, and maintain an EPW camp system. Under some circumstances, particularly during MOOTW, the JFC may designate another component commander to be responsible for the EPW camp system. The subordinate joint force J-2 establishes a JIDC for follow-on exploitation. The establishment (when, where, and how) of the JIDC is highly situation dependent, with the main factors being the geographic nature of the JOA, the type and pace of military operations, the camp structure, and the number and type of the sources. The JIDC may be a central site where appropriate EPW are segregated for interrogation, or it may be more of a clearinghouse operation for dispatch of interrogators or debriefers to other locations.

- **Organization.** The JIDC interrogation and debriefing activities are managed by the subordinate joint force HUMINT staff section or HOC. The HOC will coordinate with the TFCICA within the J-2X for CI augmentation for exploitation of those personnel of CI interest, such as civil and/or military leadership, intelligence or political officers and terrorists. The staff is augmented by deployed DHS personnel, linguists and, as required, component personnel. The HUMINT appendix of Annex B (Intelligence) to the OPLAN or CONPLAN contains JIDC planning considerations.

- **Responsibilities.** Service component interrogators collect tactical intelligence from EPWs based on joint force J-2 criteria. EPWs (i.e., senior level EPWs) are screened by the components and those of further intelligence potential are identified and processed for follow-on interrogation and debriefing by the JIDC to satisfy theater strategic and operational requirements. In addition to EPW, the JIDC may also interrogate civilian detainees, and debrief refugees as well as other non-prisoner sources for operational and strategic information.

Intentionally Blank

APPENDIX H
INTELLIGENCE CYCLE EXECUTION RESPONSIBILITIES

The intelligence cycle execution responsibilities for the Joint Staff J-2, combatant command J-2, subordinate joint force J-2, subordinate joint force components and the Military Services are depicted below.

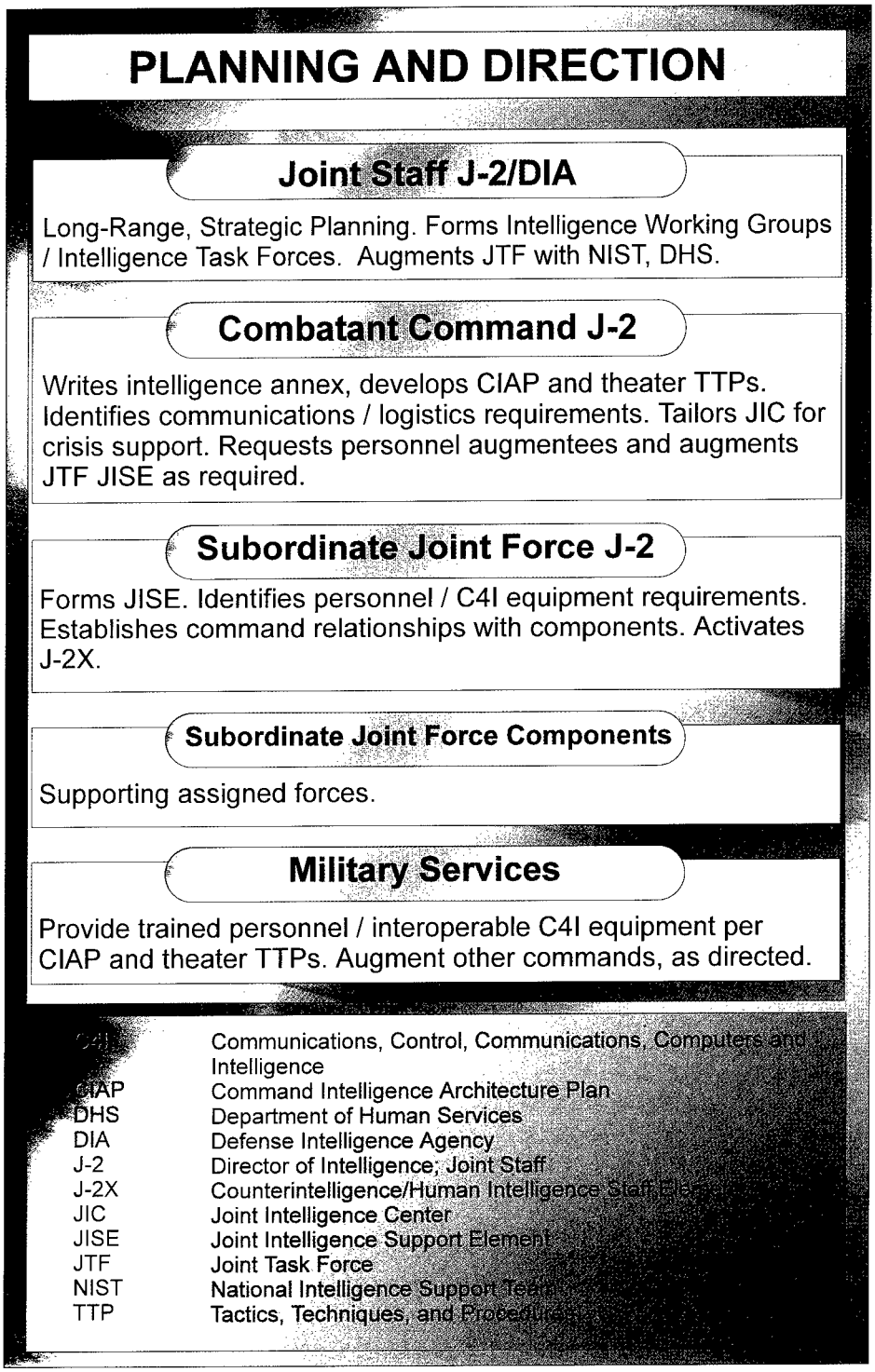


Figure H-1. Planning and Direction

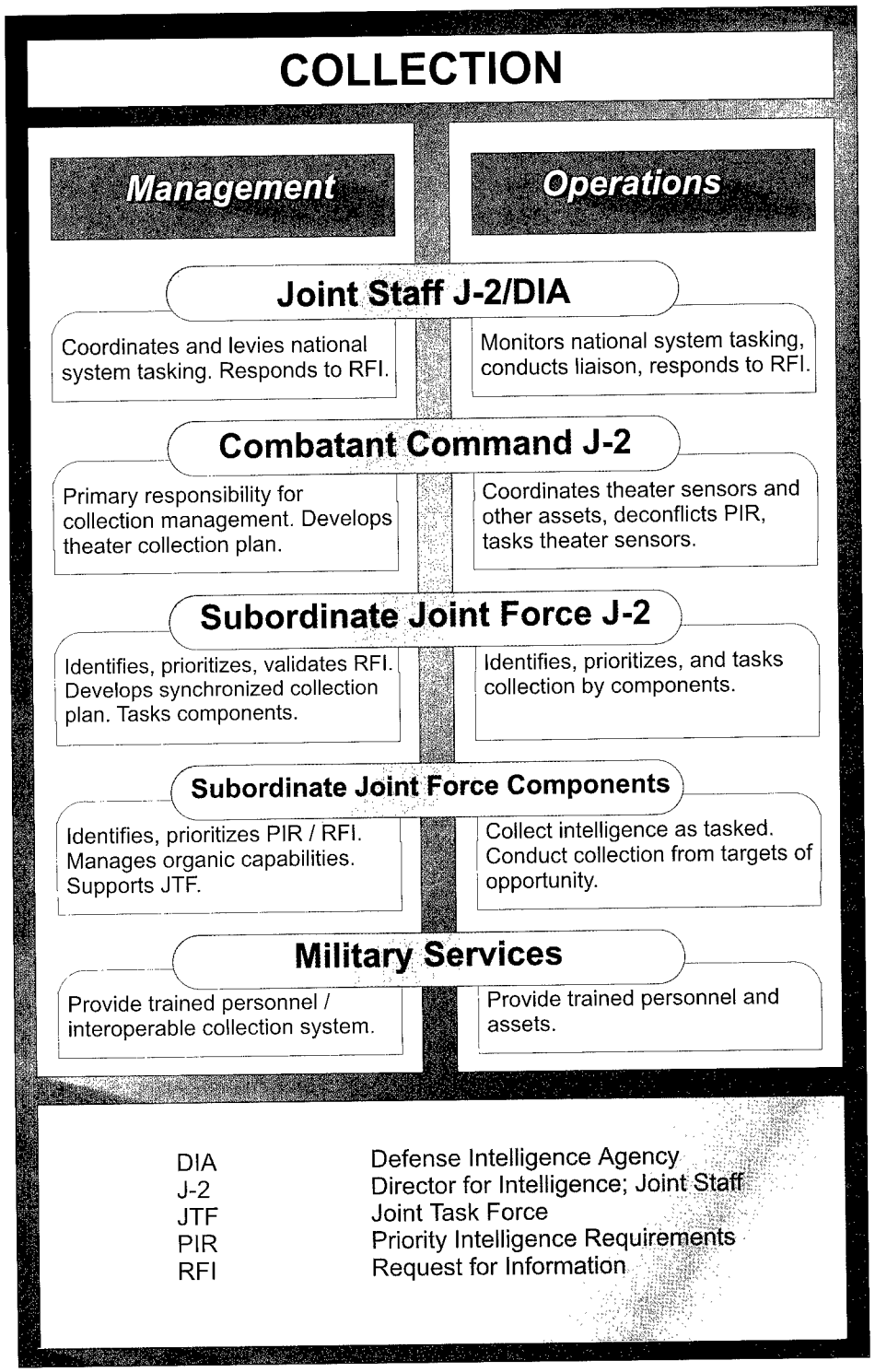


Figure H-2. Collection

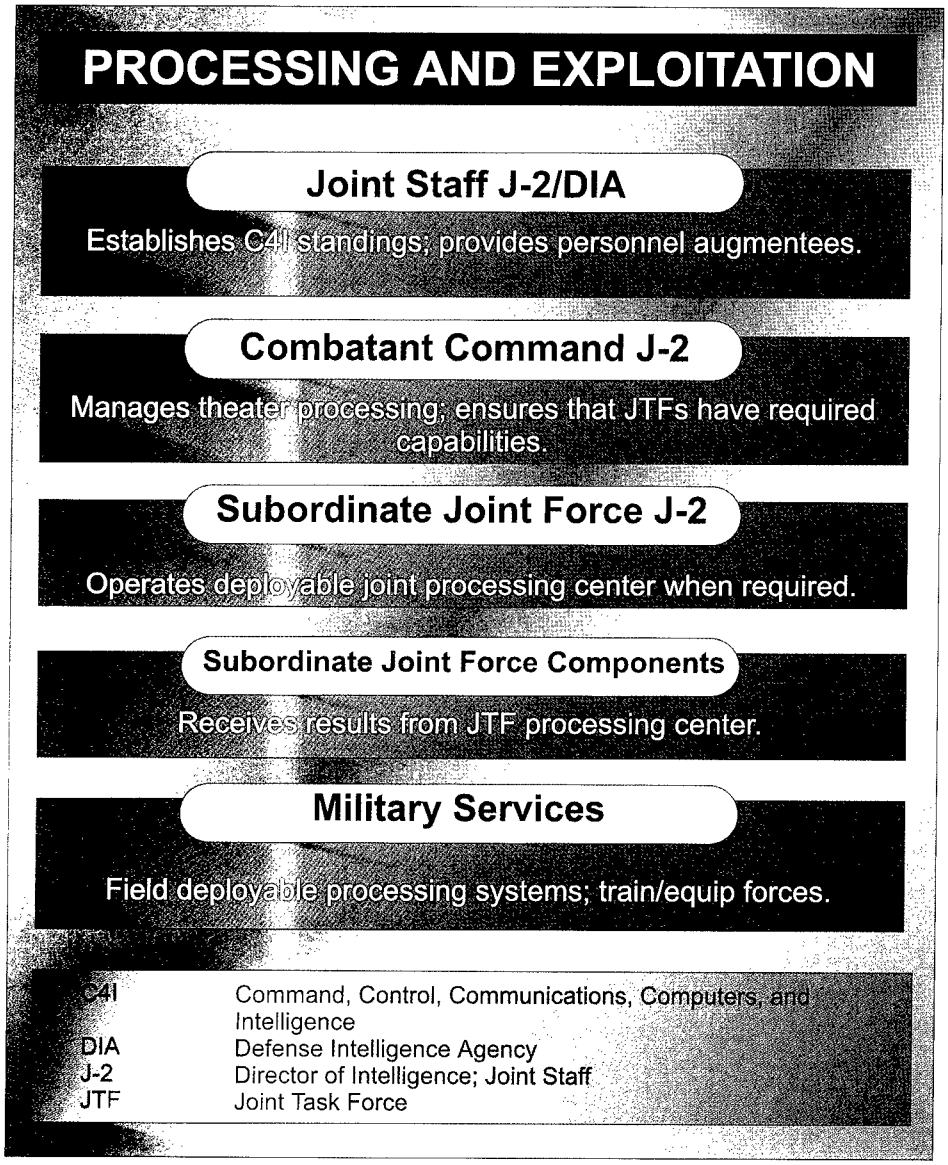


Figure H-3. Processing and Exploitation

Figure H-4. Production - Part One

PRODUCTION - PART TWO

	Indications & Warning (I&W)	Current Intelligence	General Military Intelligence	Target Intelligence	Science & Technology
Subordinate Joint Force J-2	*I&W consumers; monitors / reports*	*Mission specific intelligence; prioritizes request for intelligence*	*User of general military intelligence; tailors to joint task force focus*	*Collates operational battle damage assessment; target analysis; target development; target nominal*	*Executes technical intelligence mission in the operational area*
Subordinate Joint Force Components	*I&W consumers; monitors / reports*	*Customers; provide request for intelligence to joint task force joint intelligence support element*	*Intelligence Production Schedule*	*Report mission battle damage assessment; target analysis deconfliction; target developing; target nominal weaponeering*	*Provide technical intelligence collection requirements to forces*
Military Services	*I&W consumers; train personnel in defense I&W system*	*Customers; augment National Military Joint Intelligence Center*	*DPP participants; augment joint intelligence center production*	*Train target personnel; provide specialized functional products*	*Manage scientific and technical centers; provide personnel augmentees to joint task force; provide specialized analysis*

Figure H-4. Production - Part Two

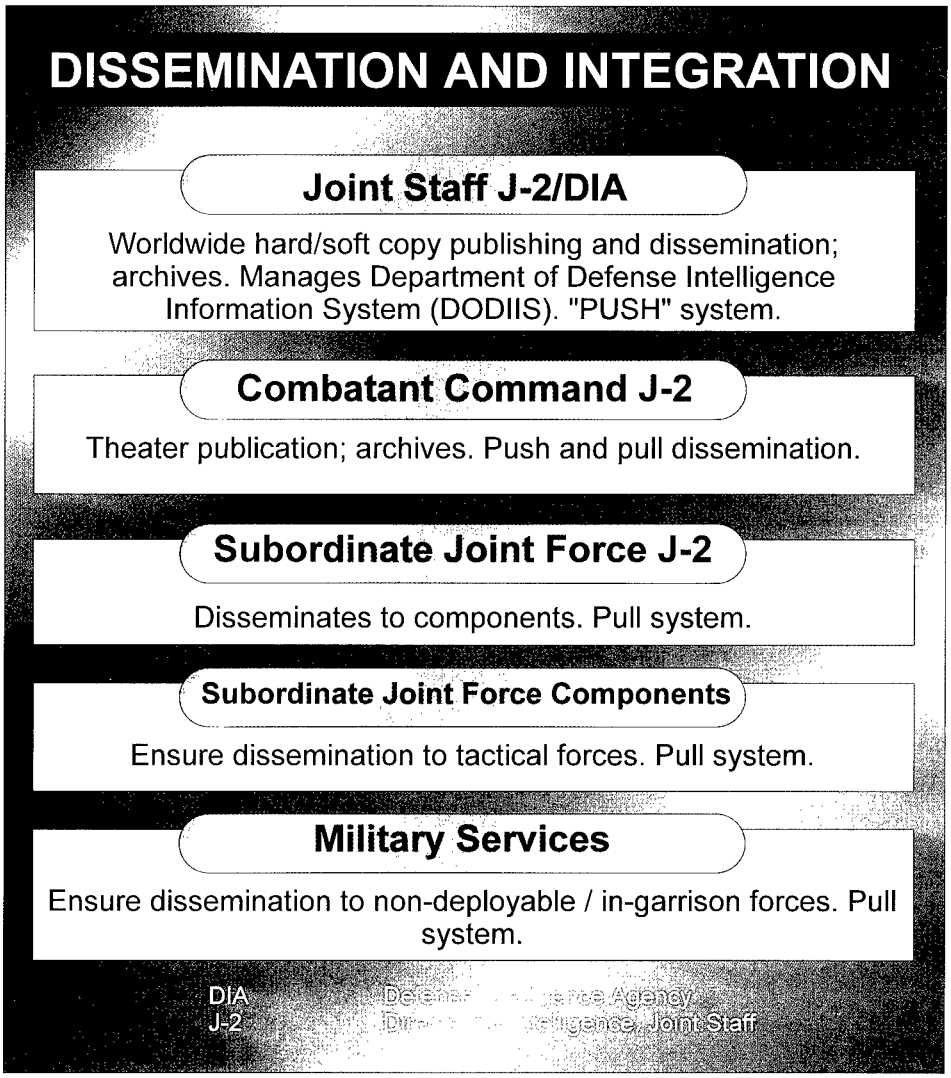


Figure H-5. Dissemination and Integration

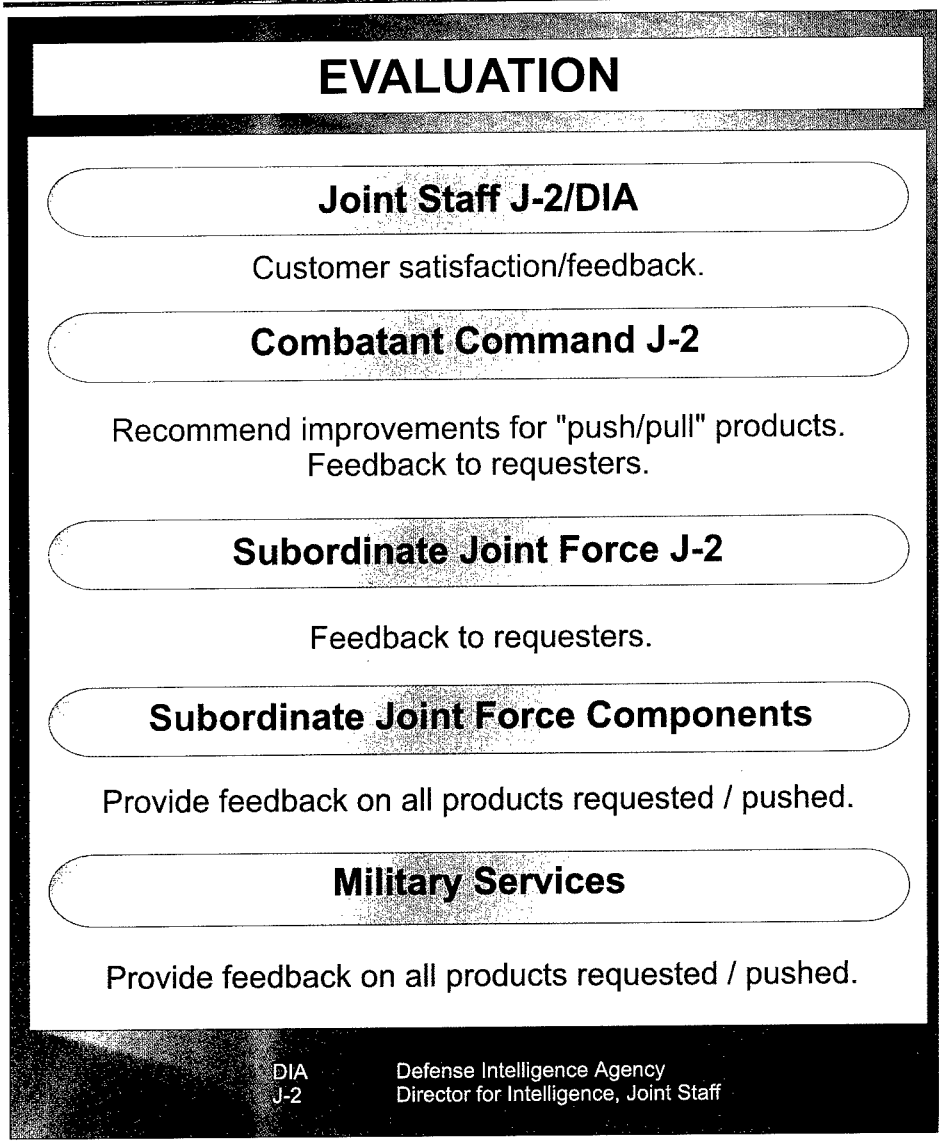


Figure H-6. Evaluation

APPENDIX J
REFERENCES

The development of Joint Pub 2-01 is based upon the following primary references.

1. National Security Act of 1947, as amended.

2. Title 10, United States Code Armed Forces, as amended.

3. Goldwater-Nichols Department of Defense Reorganization Act of 1986.

4. Executive Order 12333, "United States Intelligence Activities."

5. Executive Order 12958, "Classified National Security Information."

6. Joint Pub 1, "Joint Warfare of the Armed Forces of the United States."

7. Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)."

8. Joint Pub 1-0, "Doctrine for Personnel Support to Joint Operations."

9. Joint Pub 1-01, "Joint Publications System, Joint Doctrine and Joint Tactics, Techniques, and Procedures Development Program."

10. Joint Pub 1-02, "DOD Dictionary of Military and Associated Terms."

11. Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations."

12. Joint Pub 2-01.1, "Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting."

13. Joint Pub 2-01.2, "Joint Doctrine, and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations."

14. Joint Pub 2-02, "National Intelligence Support to Joint Operations."

15. Joint Pub 3-0, "Doctrine for Joint Operations."

16. Joint Pub 5-0, "Doctrine for Planning Joint Operations."

17. Joint Pub 5-00.2, "Joint Task Force Planning Guidance and Procedures."

18. Joint Pub 6-0, "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations."

19. Joint Pub 6-02, "Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems."

20. NDP-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations." (Short Title: National Defense Policy)

21. DOD 5200.2-R, "DOD Personnel Security Program."

22. DOD Directive S-5210.36, "Provision of DOD Sensitive Support to DOD Components and Other Departments and Agencies of the US Government."

23. DOD Directive 5205.1, "Acquisition and Reporting of Information Relating to National Security."

24. DOD Directive 5230-11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations."

25. DOD Directive 5240.1, "DOD Intelligence Activities."

26. DOD-0000-151-YR, "DOD Intelligence Production Program."

27. DOD-0000-151A-YR, "DOD Intelligence Production Program: Production Responsibilities" (U).

28. DOD-0000-151B-YR, "DOD Intelligence Production Program: Production Priorities" (U)

29. DOD-0000-151C-YR, "DOD Intelligence Production Program: Production Procedures" (U)

30. DOD S-5105.21-M-1, "Sensitive Compartmented Information Administrative Security Manual."

31. DCID 1/7, "Security Controls on the Dissemination of Intelligence Information."

32. DCID 1/21, "Physical Security Standards for SCIFs."

33. DCID 5/1, "Espionage and Counterintelligence Activities Abroad."

34. DCID 5/6, "Intelligence Disclosure Policy."

35. DCS-2600-5345-92, "DIA Guide to Foreign Disclosure."

36. DIAM 58-5, "Imagery Processing, Exploitation, Production, Reporting and Dissemination."

37. DIAM 58-8, "Measurement and Signature Intelligence (MASINT) User's Guide."

38. DIAM 58-11, "DOD Human Intelligence (HUMINT) Policies and Procedures."

39. DIAM 58-12, "DOD Human Intelligence (HUMINT) Management System."

40. DIAM 58-17, "Defense Signals Intelligence (SIGINT) Requirements Manual."

41. MJCS-51-88, "Doctrine for Intelligence Support to Joint Operations."

42. MCM-15-94, "Memorandum of Agreement Concerning CIA Support to US Military Forces."

43. CJCSI 1301.01, "Policy and Procedures to Assign Individuals to Meet Combatant Command Mission Related Temporary Duty Requirements."

44. CJCSI 3210.01, "Joint Information Warfare Policy."

45. CJCSI 5221.01, "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations."

46. CJCSI 6110.01, "CJCJ-Control Tactical Communications Assets."

47. CJCSM 3122.02, "Manual for Time-Phased Force and Deployment Data (TPFDD) Development and Deployment Execution."

48. CJCSM 3122.03, "Joint Operation Planning and Execution System Vol II: (Planning Formats and Guidance)."

49. CJCSM 3122.04, "Joint Operation Planning and Execution System, Vol II: (Supplemental Planning and Execution Formats and Guidance)."

50. "Joint-Service Tactical Exploitation of National Systems (J-TENS) Manual."

51. "Handbook of the National SIGINT Requirements System."

52. IPSG/INCA-133, "Communications Handbook for Intelligence Planners."

53. USIS Directive 2-0, "Imagery Processing, Exploitation, and Delivery Policy."

54. Public Law 585, Atomic Energy Act of 1954, as amended.

Intentionally Blank

APPENDIX K
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to the Joint Warfighting Center, Attn: Doctrine Division, Fenwick Road, Bldg 96, Fort Monroe, VA 23651-5000. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and the Joint Staff doctrine sponsor for this publication is the Director for Intelligence (J-2).

3. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J2-J2P/J7-JDD//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDD, 7000 Joint Staff Pentagon, Washington, D.C. 20318-7000.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

4. Distribution

a. Additional copies of this publication can be obtained through Service publication centers.

b. Only approved pubs and test pubs are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attache Office) to DIA Foreign Liaison Office, PSS, Room 1A674, Pentagon, Washington, D.C. 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

By Military Services:

Army:	US Army AG Publication Center 2800 Eastern Boulevard Baltimore, MD 21220-2898
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Marine Corps Logistics Base Albany, GA 31704-5000
Coast Guard:	Coast Guard Headquarters, COMDT (G-OPD) 2100 2nd Street, SW Washington, D.C. 20593-0001

d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R.

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

AAA	anti-aircraft artillery
ADP	automated data processing
AIG	addressee indicator group
AOR	area of responsibility
AUTODIN	Automatic Digital Network
BDA	battle damage assessment
C2	command and control
C2W	command and control warfare
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
CA	combat assessment
CAP	crisis action planning
CCD	camouflage, concealment, and deception
CD-ROM	compact disk - read only memory
CEE	captured enemy equipment
CI	counterintelligence
CIA	Central Intelligence Agency
CIAP	Command Intelligence Architecture/Planning Program
CINC	commander of a combatant command; commander in chief
CIO	Central Imagery Office
CISO	Counterintelligence Support Officer
CJCS	Chairman of the Joint Chiefs of Staff
COA	course of action
COLISEUM	Community On-Line Intelligence System for End-Users and Managers
COM	collection operations management
COMINT	communications intelligence
COMSEC	communications security
CONPLAN	operation plan in concept format
CONUS	continental United States
CRM	collection requirements management
CSAR	combat search and rescue
CSE	client server environment
CSG	cryptologic support group
CSS	Central Security Service
DCI	Director, Central Intelligence
DCID	Director, Central Intelligence Directive
DHS	Defense HUMINT Service
DI	DIA Directorate for Intelligence Production
DIA	Defense Intelligence Agency
DIDS	Defense Intelligence Dissemination System

DIN	defense intelligence network
DISA	Defense Intelligence Agency
DISN	Defense Information Systems Network
DISO	Defense Intelligence Support Office
DMA	Defense Mapping Agency
DO	DIA Directorate of Operations
DOD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DODIPC	Department of Defense Intelligence Production Community
DODIPP	Department of Defense Intelligence Production Program
DPM	Dissemination Program Manager
ELINT	electronic intelligence
EPW	enemy prisoner of war
EW	electronic warfare
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCI	ground control intercept
GI&S	geospatial information and services
GMI	general military intelligence
HOC	HUMINT Operations Cell
HSE	HUMINT support element
HUMINT	human intelligence
I&W	indications and warning
IAW	in accordance with
IDB	Integrate Data Base
IMA	individual mobilization augmentee
IMINT	imagery intelligence
IRR	individual ready reserve
IW	information warfare
J-1	Joint Manpower and Personnel Staff
J-2	Joint Intelligence Staff
J-2X	joint force J-2 CI/HUMINT staff element
J-3	Joint Operations Staff
J-4	Joint Logistics Staff
J-5	Joint Strategic Plans Staff
J-6	Joint Command, Control, Communications, and Computer (C4) Systems Staff
JC2WC	Joint Command and Control Warfare Center
JCMEC	Joint Captured Materiel Exploitation Center
JCMT	Joint Collection Management Tools
JCS	Joint Chiefs of Staff
JCSE	Joint Communications Support Element
JDEC	Joint Document Exploitation Center

JDISS	Joint Deployable Intelligence Support System
JFC	joint force commander
JIC	Joint Intelligence Center
JIDC	Joint Interrogation and Debriefing Center
JIPB	joint intelligence preparation of the battlespace
JISE	Joint Intelligence Support Element
JMICS	JWICS Mobile Integrated Communications System
JOA	joint operations area
JOPES	Joint Operation Planning and Execution System
JSST	Joint Space Support Team
JTF	joint task force
JTMD	joint table of mobilization and distribution
JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
LOCE	Linked Operational Intelligence Centers Europe
LOCs	lines of communications
MASINT	measurement and signature intelligence
MDITDS	Migration Defense Intelligence Threat Data System
METOC	meteorological and oceanographic
MIIDS	Military Intelligence Integrated Data System
MOOTW	military operations other than war
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NCA	National Command Authorities
NCR	National Cryptologic Representative
NCSE	NIST Communications Support Element
NDP	National Disclosure Policy
NDPC	National Disclosure Policy Committee
NIST	National Intelligence Support Team
NMJIC	National Military Joint Intelligence Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
OB	order of battle
OPLAN	operation plan
OPORD	operation order
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
OSIS	Open Source Information System
PGM	precision-guided munitions
PIR	priority intelligence requirements
POC	point of contact
POL	petroleum, oil, and lubricants

PR	production requirement
PSYOP	psychological operations
RFI	request for information
RMS	Requirements Management System
S&TI	scientific and technical intelligence
SAM	surface-to-air missile
SATCOM	satellite communications
SCI	sensitive compartmented information
SCIF	SCI facility
SIGINT	signals intelligence
SII	statement of intelligence interest
SIO	senior intelligence officer
SIPRNET	SECRET Internet Protocol Router Network
SIR	specific information requirement
SOF	special operations forces
SOIC	senior official of the Intelligence Community
SPP	Shared Production Program
SSM	surface-to-surface missile
SSO	Special Security Office(r)
STEP	standard tactical entry point
TBM	theater ballistic missile
TENCAP	Tactical Exploitation of National Capabilities Program
TFCICA	Task Force Counterintelligence Coordinating Authority
TIP	target intelligence package
TPFDD	time-phased force and deployment data
TPFDL	time-phased force and deployment list
TSWA	temporary secure working areas
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
UN	United Nations
US	United States
USSPACECOM	US Space Command
USTRANSCOM	US Transportation Command
UW	unconventional warfare
VO	Validation Office
WAN	wide-area network
WMD	weapons of mass destruction

PART II—TERMS AND DEFINITIONS

all-source intelligence. 1. Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (Joint Pub 1-02)

battlespace. The commander's conceptual view of the environment and factors which must be understood to successfully apply combat power, protect the force, and complete the mission. Battlespace encompasses the surface, subsurface, endoatmosphereic, and extoatmospheric spheres of a particular geographic area. It also includes the electromagnetic spectrum, cyperspace, and human psychological aspects of military operations. The dimensions of a command's battlespace are dictated by its mission, its capabilities, and the capabilities of any potential adversaries. A command's battlespace embodies its operational area and area of interest. (This term and its definition are applicable only in the context of this pub and cannot be referenced outside this publication.)

collection asset. A collection system, platform, or capability that is supporting, assigned or attached to a particular commander. (Approved for inclusion in the next edition of Joint Pub 1-02.)

collection management. The process of converting intelligence requirements into collection requirements, establishing priorities, and tasking or coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required. (This term and its definition modifies the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

collection management authority. Constitutes the authority to establish, prioritize and validate theater collection requirements, establish sensor tasking guidance and develop theater collection plans. Also called CMA. (Approved for inclusion in the next edition of Joint Pub 1-02.)

collection manager. An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. Also called CM. (Approved for inclusion in the next edition of Joint Pub 1-02.)

collection operations management. The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. Also called COM. (Joint Pub 1-02)

collection requirements management. The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either the direct tasking of assets over which the collection manager has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. Also called CRM. (This term and its definition

modifies the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

collection resource. A collection system, platform, or capability that is not assigned or attached to a specific unit or echelon which must be requested and coordinated through the chain of command. (Approved for inclusion in the next edition of Joint Pub 1-02.)

combat intelligence. That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (Joint Pub 1-02)

command and control warfare. The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information warfare in military operations and is a subset of information warfare. Command and control warfare applies across the range of military operations and all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade or destroy the friendly C2 system. (Joint Pub 1-02)

communications intelligence. Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT. (Joint Pub 1-02)

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (Joint Pub 1-02)

data base. Information that is normally structured and indexed for user access and review. Data bases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (Joint Pub 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Joint Pub 1-02)

Defense Information Systems Network. Integrated network, centrally managed and configured to provide long-haul information transfer services for all DOD activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services. Also called DISN. (Approved for inclusion in the next edition of Joint Pub 1-02.)

Department of Defense Intelligence Information System. The aggregation of DOD personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and intelligence information to military commanders and national-level decisionmakers. Also called DODIIS. (Joint Pub 1-02)

electronic intelligence. Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (This term and its definition modifies the existing term "electronics intelligence" and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

estimate. 1. An analysis of a foreign situation, development, or trend that identifies its major elements, interprets the significance, and appraises the future possibilities and the prospective results of the various actions that might be taken. 2. An appraisal of the capabilities, vulnerabilities, and potential courses of action of a foreign nation or combination of nations in consequence of a specific national plan, policy, decision, or contemplated course of action. 3. An analysis of an actual or contemplated clandestine operation in relation to the situation in which it is or would be conducted in order to identify and appraise such factors as available and needed assets and potential obstacles, accomplishments, and consequences. See also intelligence estimate. 4. In air intercept, a code meaning, "Provide a quick estimate of the height/depth/range/size of designated contact," or "I estimate height/depth/range/size of designated contact is _____." (Joint Pub 1-02)

force protection. Security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combatting terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (Joint Pub 1-02)

foreign instrumentation signals intelligence. Technical and intelligence information derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include, but are not limited to, telemetry, beaconry, electronic interrogators, and video data links. Also called FISINT. (This term and its definition modifies the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

general military intelligence. Intelligence concerning the (1) military capabilities of foreign countries or organizations or (2) topics affecting potential US or allied military operations, relating to the following subjects: armed forces capabilities, including order of battle, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness; area and terrain intelligence, including urban areas, coasts and landing beaches, and meteorological, oceanographic, and geological intelligence; transportation in all modes; military materiel production and support industries; military and civilian C4 systems; military economics, including foreign military assistance; insurgency and terrorism; military-political-sociological intelligence; location, identification, and description of military-related installations; government control; escape and evasion; and threats and forecasts. (Excludes scientific and technical intelligence). Also called GMI. (This term and its definition modifies the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

Global Command and Control System. Highly mobile, deployable command and control system supporting forces for joint and multinational operations across the range of military operations, any time and anywhere in the world with compatible, interoperable, and integrated command, control, communications, computers, and intelligence systems. Also called GCCS. (Approved for inclusion in the next edition of Joint Pub 1-02.)

geospatial information and services. The collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the earth's surface. These data are used for military planning, training, and operations including navigation, mission planning, rehearsal, modeling, simulation, and precise targeting. Geospatial information provides the basic framework for battlespace visualization. It is information produced by multiple sources to common interoperable data standards. It may be presented in the form of printed maps, charts, and publications; in digital simulation and modeling data bases; in photographic form; or in the form of digitized maps and charts or attributed centerline data. Geospatial services include tools that enable users to access and manipulate data, and also includes instruction, training, laboratory support, and guidance for the use of geospatial data. Also called GI&S. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 2-03)

human intelligence. A category of intelligence derived from information collected and provided by human sources. Also called HUMINT. (Joint Pub 1-02)

imagery intelligence. Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called IMINT. (Joint Pub 1-02)

indications and warning. Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. (Joint Pub 1-02)

information warfare. Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks. (Joint Pub 1-02)

intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (Joint Pub 1-02)

intelligence cycle. The process by which information is converted into intelligence and made available to users. There are six phases in the cycle: a. planning and direction — Determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies b. collection — Acquisition of information and the provision of this information to processing elements. c. processing and exploitation — Conversion of collected information into forms suitable to the production of intelligence. d. production — Conversion of processed information into intelligence through the integration, analysis, evaluation, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. e. dissemination and integration — Delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. f. evaluation — Continuous assessment of intelligence operations during each phase of the intelligence cycle to ensure that the commander's intelligence requirements are being met. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 2-0.)

intelligence discipline. A well defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are five major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence), and open source intelligence. (Approved for inclusion in the next edition of Joint Pub 1-02.)

intelligence estimate. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (Joint Pub 1-02)

intelligence operations. The variety of intelligence tasks that are carried out by various intelligence organizations and activities. Predominantly, it refers to either intelligence collection or intelligence production activities. When used in the context of intelligence collection activities, intelligence operations refer to collection, processing, exploitation, and reporting of information. When used in the context of intelligence production activities, it refers to collation, integration, interpretation, and analysis, leading to the dissemination of a finished product. (Joint Pub 1-02)

intelligence requirement. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (Joint Pub 1-02)

intelligence system. Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decisionmakers as a basis for action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks. (Joint Pub 1-02)

interoperability. 1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. The condition achieved among communications-electronics systems or items of

communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (Joint Pub 1-02)

J-2X. Umbrella organization consisting of the HUMINT Operations Cell and the Task Force Counterintelligence Coordinating Authority. The J-2X is responsible for coordination and deconfliction of all human source related activity. (Approved for inclusion in the next edition of Joint Pub 1-02.)

joint captured materiel exploitation center. Physical location for deriving intelligence information from captured enemy materiel. It is normally subordinate to the joint force/ J-2. Also called JCMEC. (Joint Pub 1-02)

joint deployable intelligence support system. A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called JDISS. (Joint Pub 1-02)

joint doctrine. Fundamental principles that guide the employment of forces of two or more Services in coordinated action toward a common objective. It will be promulgated by the Chairman of the Joint Chiefs of Staff, in coordination with the combatant commands, Services, and Joint Staff. (Joint Pub 1-02)

joint document exploitation center. Physical location for deriving intelligence information from captured enemy documents. It is normally subordinate to the joint force/J-2. Also called JDEC. (Approved for inclusion in the next edition of Joint Pub 1-02.)

joint force. A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (Joint Pub 1-02)

joint intelligence architecture. A dynamic, flexible structure that consists of the National Military Joint Intelligence Center, the theater joint intelligence centers, and subordinate joint force joint intelligence support elements. This architecture encompasses automated data processing equipment capabilities, communications and information requirements, and responsibilities to provide national, theater and tactical commanders with the full range of intelligence required for planning and conducting operations. (This term and its definition modifies the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

joint intelligence center. The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. Also called JIC. (Joint Pub 1-02)

joint intelligence preparation of the battlespace. The analytical process used by joint intelligence organizations to produce intelligence assessments, estimates and other intelligence products in support of the joint force commander's decision making process. It is a continuous process that includes defining the total battlespace environment; describing battlespace characteristics; evaluating the adversary; and determining and describing adversary courses of actions. The process is used to analyze the surface, sub-surface,

endoatmospheric, exoatmospheric, electromagnetic, cyberspace, and human dimensions of the environment and to determine an opponent's capabilities to operate in each. Joint intelligence preparation of the battlespace products are used by other staff elements in preparing their estimates and are also applied during the analysis and selection of friendly courses of action. Also called JIPB. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 2-0.)

joint intelligence doctrine. Fundamental principles that guide the preparation of intelligence and the subsequent provision of intelligence to support military forces of two or more Services employed in coordinated action. (Joint Pub 1-02)

joint intelligence support element. A subordinate joint force forms a joint intelligence support element as the focus for intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called JISE. (Approved for inclusion in the next edition of Joint Pub 1-02.)

joint interrogation and debriefing center. Physical location for the exploitation of intelligence information from enemy prisoners of war and other non-prisoner sources. It is normally subordinate to the joint force/J-2. Also called JIDC. (Approved for inclusion in the next edition of Joint Pub 1-02.)

Joint Worldwide Intelligence Communications System. The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (Joint Pub 1-02)

measurement and signature intelligence. Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. Also called MASINT. (This term and its definition modifies the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

medical intelligence. That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information which is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors. (Joint Pub 1-02)

Military Intelligence Integrated Data System/Integrated Data Base. An architecture for improving the manner in which military intelligence is analyzed, stored, and disseminated. The Integrated Data Base (IDB) forms the core automated data base for the Military Intelligence Integrated Data System (MIIDS) program and integrates the data in the installation, order of battle, equipment, and selected electronic warfare and command, control, and communications files. The IDB is the national-level repository for the general military intelligence information available to the entire Department of Defense

Intelligence Information System community and maintained by DIA and the commands. The IDB is kept synchronized by system transactions to disseminate updates. Also called MIIDS/ IDB. (Approved for inclusion in the next edition of Joint Pub 1-02.)

open-source intelligence. Information of potential intelligence value that is available to the general public. Also called OSINT. (Joint Pub 1-02)

operational intelligence. Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations. (Joint Pub 1-02)

operation order. A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. Also called OPORD. (Joint Pub 1-02)

operation plan. Any plan, except for the Single Integrated Operation Plan, for the conduct of military operations. Plans are prepared by combatant commanders in response to requirements established by the Chairman of the Joint Chiefs of Staff and by commanders of subordinate commands in response to requirements tasked by the establishing unified commander. Operation plans are prepared either in a complete format (OPLAN), or as a concept plan (CONPLAN). The CONPLAN can be published with or without a time-phased force and deployment data (TPFDD) file. a. OPLAN—An operation plan for the conduct of joint operations that can be used as a basis for development of an operation order (OPORD). An OPLAN identifies the forces and supplies required to execute the CINC's Strategic Concept and a movement schedule of these resources to the theater of operations. The forces and supplies are identified in TPFDD files. OPLANs will include all phases of the tasked operation. The plan is prepared with the appropriate annexes, appendixes, and TPFDD files as described in the Joint Operation Planning and Execution System manuals containing planning policies, procedures, and formats. Also called OPLAN. b. CONPLAN—An operation plan in an abbreviated format that would require considerable expansion or alteration to convert it into an OPLAN or OPORD. A CONPLAN contains the CINC's Strategic Concept and those annexes and appendixes deemed necessary by the combatant commander to complete planning. Generally, detailed support requirements are not calculated and TPFDD files are not prepared. Also called CONPLAN. c. CONPLAN with TPFDD—A CONPLAN with TPFDD is the same as a CONPLAN except that it requires more detailed planning for phased deployment of forces. (Joint Pub 1-02)

priority intelligence requirements. Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. (Joint Pub 1-02)

reconnaissance. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (Joint Pub 1-02)

request for information. 1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the

theater command's procedures. 2. The National Security Agency/Central Security Service uses this term to state ad hoc signals intelligence requirements. Also called RFI. (Approved for inclusion in the next edition of Joint Pub 1-02.)

Requirements Management System. A system for the management of theater and national imagery collection requirements. Provides automated tools for users in support of submission, review, and validation of imagery nominations as requirements to be tasked on national or DOD imagery collection, production, and exploitation resources. Also called RMS. (Approved for inclusion in the next edition of Joint Pub 1-02.)

scientific and technical intelligence. The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the research and development related thereto, and the production methods employed for their manufacture. (Joint Pub 1-02)

SECRET Internet Protocol Router Network. Worldwide SECRET level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called SIPRNET. (Approved for inclusion in the next edition of Joint Pub 1-02.)

sensitive compartmented information facility. An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. Also called SCIF. (Approved for inclusion in the next edition of Joint Pub 1-02.)

signals intelligence. 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. (Joint Pub 1-02)

situation assessment. Assessment produced by combining military geography, weather, and threat data to provide a comprehensive projection of the situation for the decisionmaker. (Joint Pub 1-02)

strategic intelligence. Intelligence that is required for the formulation of military strategy, policy, and plans and operations at national and theater levels. (This term and its definition modifies the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

surveillance. The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (Joint Pub 1-02)

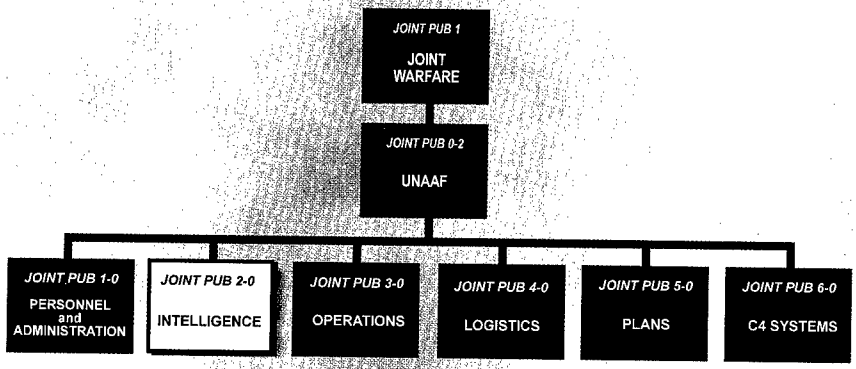
tactical intelligence. Intelligence that is required for planning and conducting tactical operations. (Joint Pub 1-02)

targeting. 1. The process of selecting targets and matching the appropriate response to them, taking account of operational requirements and capabilities. 2. The

analysis of enemy situations relative to the commander's mission, objectives, and capabilities at the commander's disposal, to identify and nominate specific vulnerabilities that, if exploited, will accomplish the commander's purpose through delaying, disrupting, disabling or destroying enemy forces or resources critical to the enemy. (Joint Pub 1-02)

validation. 1. A process normally associated with the collection of intelligence that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not been previously satisfied. 2. In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. (Joint Pub 1-02)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. **Joint Pub 2-01** is in the **Intelligence** series of joint doctrine publications. The diagram below illustrates an overview of the development process: